Document ID: ECHO_Guide_003
Revision: 3

Group Management & ACLs How To

Prepared by: Linnette Quick and Matt Cechini

1 Introduction

The information in this document provides an introduction to the new ACL and Group Management capabilities being developed in ECHO. As of ECHO 10.22, this functionality is available and does affect access to catalog items and provider information. The previous functionality will remain in the ECHO API and PUMP for 1 or 2 releases, but will not impact access control. The screenshots included in the following sections assume that the user has logged in and set their context to an ECHO provider. An initial set of data partner users will be granted the ability to set their context. These users may add additional users.

To review, there are two separate ACL management areas, *Provider Object ACLs* and *Catalog Item ACLs*. *Provider Object ACLs* control access to items such as provider orders, policies, groups, etc. *Catalog Item ACLs* control the visibility and orderability of all collections and granules within an ECHO provider's holdings.

In the new ACL and Group Management structure, there will no longer be a "provider role" that is assigned to users. Instead, a group named "Administrators" will be created for each provider and initially assigned permissions on all *Provider Object ACLs* along with the ability to view and order all catalog items. Only members of this provider administration group will be able to assign permissions on *Provider Object ACLs* to other groups. This allows for the creation of group roles, but protects the ability to manage access to provider information. The ability to manage *Catalog Item ACLs*, however, is not limited to the provider administrators. This management capability can be granted to other provider groups, who may then pass on the management capability. This facilitates the creation of user services group(s) that can then manage access to catalog items, without needing to coordinate with the provider administrators.

1.1 Frequently Asked Questions

- What is a *Provider Object* – A *Provider Object* is an item associated with an ECHO provider over which the ECHO system will control permissions to create, read, update, and/or delete. For example, a provider's ordering policies are considered to be a *Provider Object.*

- What constitutes an ACL? - An ACL designates the permissions granted to groups for a specific listing of catalog items or provider objects. Provider Object ACLs are not created, only modified to add or remove assigned permissions and groups. Catalog Item ACLs are created since there is a dynamic list of identities that can be created.

- What is a Catalog Item ACL? – A catalog item ACL is an ACL that is associated with a set of granules and/or collections which have been identified by the available metadata values. Catalog Item ACLs, similar to Provider Object ACLs, may exist without any groups being assigned permissions.

- How are permissions to view and order collections or granules managed? – Permissions to view and order collections and/or granules are independently configured. This allows for dataset discovery without granule discovery in the event that a provider has such a need. This also allows for separate orderability permissions for collections vs. granules.

- What happened to my old groups? – During the migration to the new Group Management capability, ECHO operations brokered the listing of groups which should be migrated into the new provider groups. The original ECHO groups still exist and will continue to function until the new functionality is made effective.

- Why can't I see any groups? – In order to view groups for your provider, you must be in a group that has been assigned the *Read* permission on the *Group* provider object.

- How is the *provider role* handled? – Previously, users must be granted to *provider role* in order to view provider information and manage ACLs. In the new capability, users must first be in a member of a group to which the read permission on the *Provider Context* object has been assigned. This will allow a user to "set their context" to a provider. The ability to perform additional activities will be dictated by the other permissions granted to groups the user is a member of.

- Why are guest and registered users handled separately? – As a part of the new design, ECHO will treat guest users and registered users as mutually exclusive groups. Therefore, it is important to assign permissions to each group independently.

2 Group Management

2.1 Adding Provider Groups

The following section describes the steps necessary for creating new provider groups.

2.1.1 Design Overview

In order to view all groups for a provider, a user must be in a group that has been given the *Read* privilege on the "Groups" provider object. A separate ACL for each provider group will be used to allow users to update or delete a group. In order to update or delete a group, a user must be in a group that has been given the *Update* and *Delete* permissions on the "Group Management" ACL associated with the desired group.

2.1.2 User Interface

From the "Provider Context" tab, select "Data Management", and then select "Provider Groups". The screen shown in Figure 1 will be displayed. If the user has been granted permissions to view groups, a listing of all provider groups will be shown. The user may press the "View" button to see more details about the group. Groups for which the current user has "Group Management" ACL permissions will have an additional "Update" and "Delete" button, allowing them to modify group membership or delete a group. The "[group not accessible]" text will be displayed when the group is managed by a group that the current user does not have access. Specifically, the ECHO Operations System Administrator group. Press the "Add New Group" button to add a new group. The screen shown in Figure 2 will be displayed.

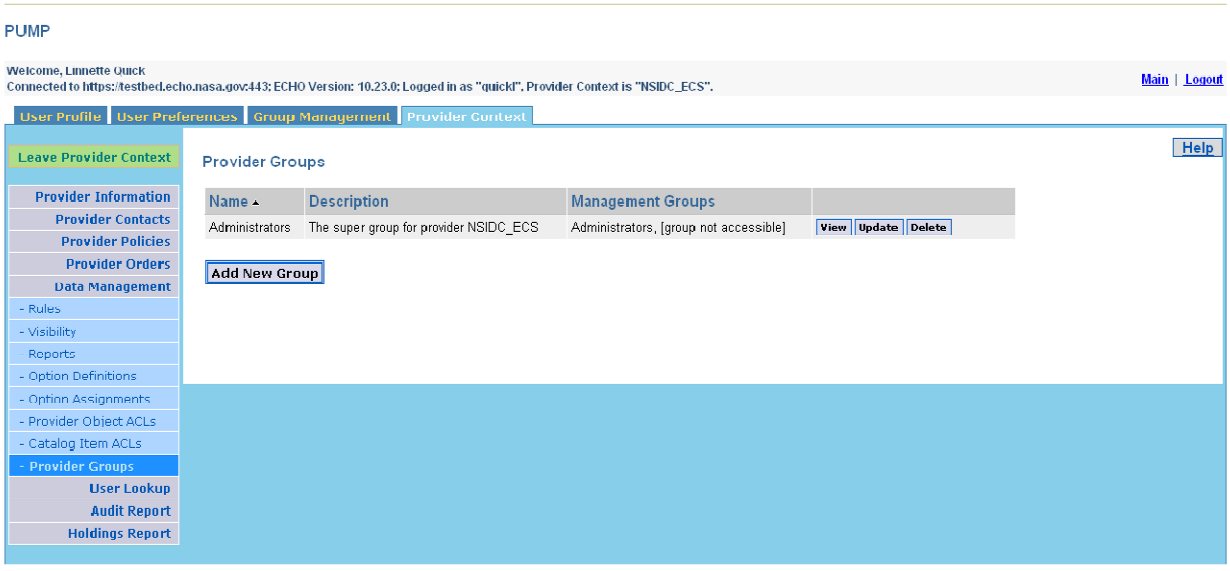


Figure 1 - Group Management - Group Listing

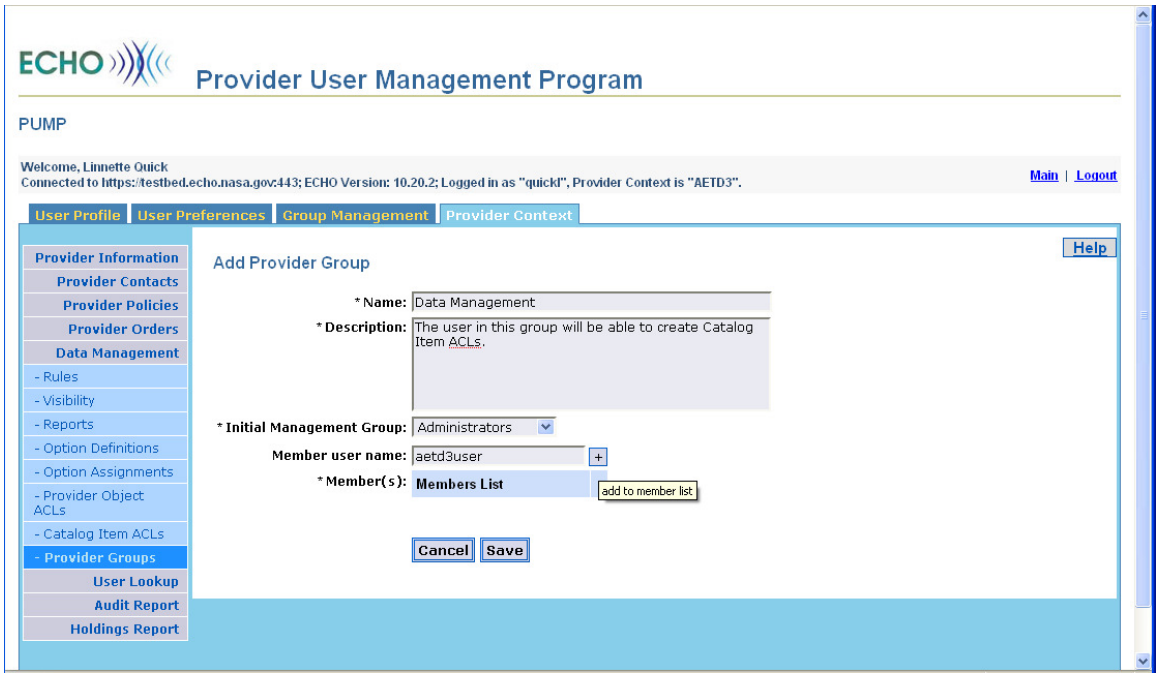


Figure 2 - Group Management - Add New Group

Required fields are indicated with an asterisk. Select the group that will manage the created group from the select list in the “Initial Management Group”. This group will be permitted to manage (update/delete) the new group. It is recommended that the Provider’s *Administrators* group be selected as the “Initial Management Group” when configuring groups that will be given permissions on Provider Object ACLs.

To add a user as a member, enter the user name in the “Member user name” field and click the '+' button to add the name to the list of group members. All changes must be finalized by clicking the 'Save' button. The user will then be returned to the groups listing screen, shown in Figure 3.

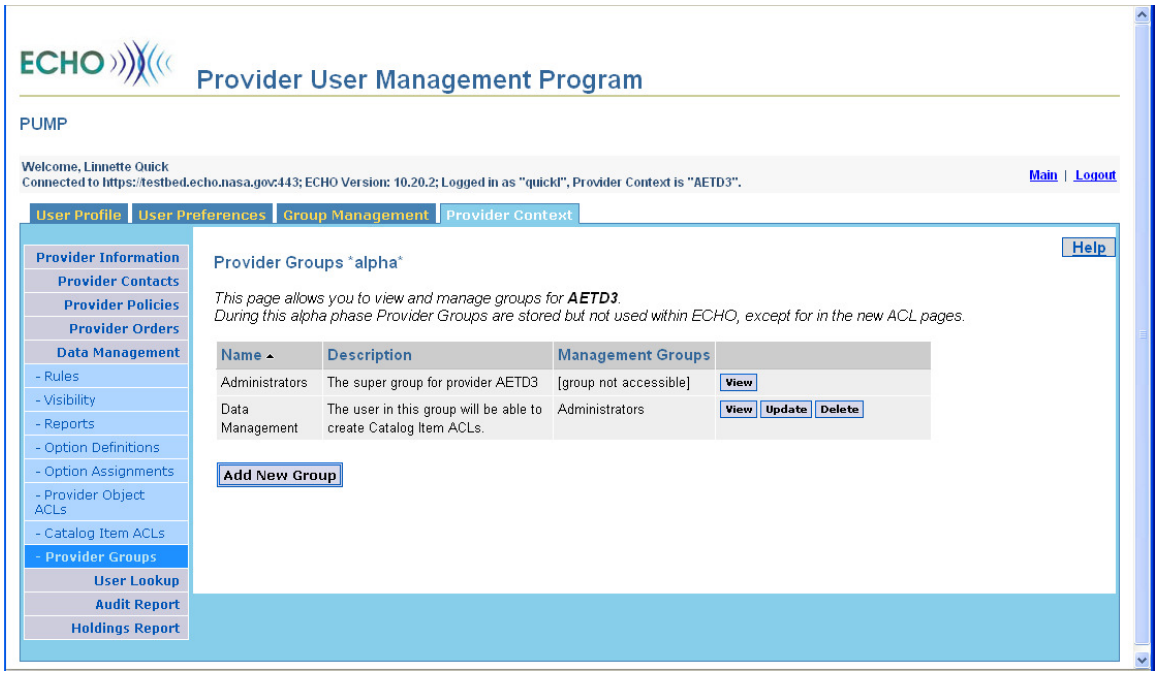


Figure 3 - Group Management - New Group Added

2.1.3 Sample Use Case

As a provider, there are two natural separations of duties: Data Management and User Services. In order to manage which team members have permissions to perform the associated tasks in these areas, you may create a user group for each role. The Provider Administrators may then add members to those groups and assign the relevant permissions. We suggest that the permissions to update or delete these groups remain with the Provider Administrators only.

Providers will also want to manage access to data with non-public access. Groups may be created for each logical distinction of user type (e.g. science teams, internal testers, special customers, etc). These groups will not be granted any permissions to provider object ACLs, but instead will be granted permissions to view and order catalog items. This is discussed in a later section.

2.2 Updating Existing Provider Groups

From the “Provider Context” tab, select “Data Management”, and then select “Provider Groups”. The screen shown in Figure 1 will be displayed. Select “Update” to modify group membership. The screen shown in Figure 4 will be displayed. If you do not see the “Update” button, next to a specific group, then that means you are not a part of a group with permissions to perform updates. You will need to request that you be granted permissions to do so.

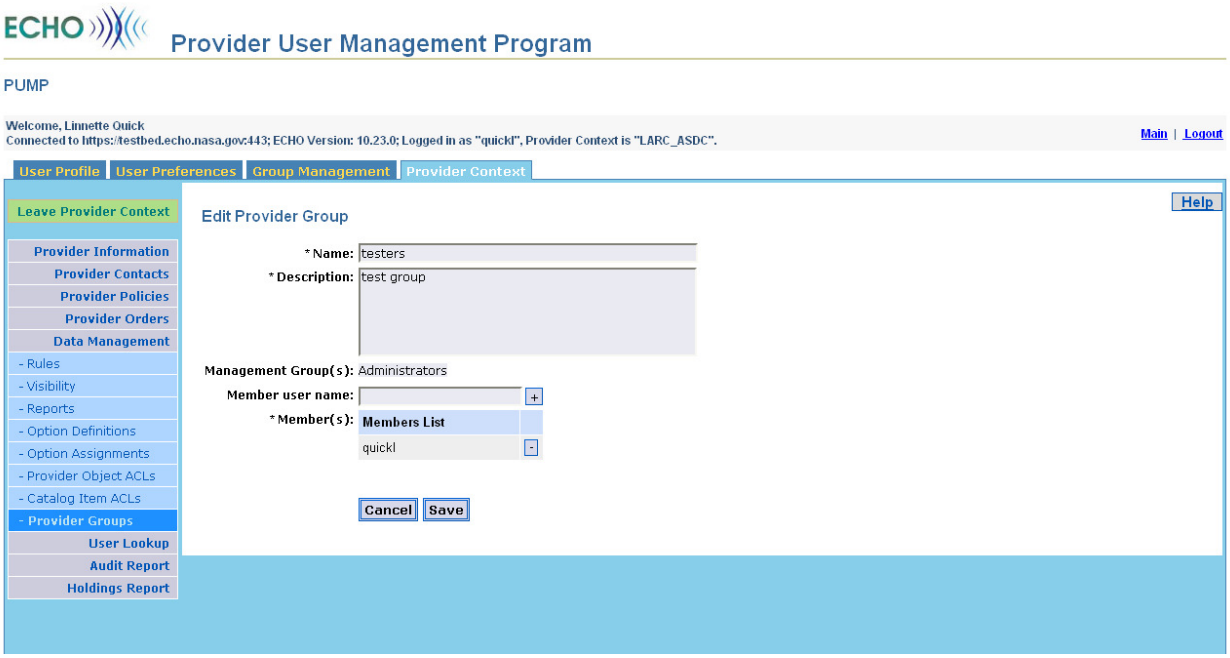


Figure 4 - Group Management - Update Group

Required fields are indicated with an asterisk. To add a user as a member enter the user name in the “Member user name” field and click the '+' button to add the name to the list of group members. To delete a user click the '-' button next to the user name. All changes must be finalized by clicking the 'Save' button. The user will then be returned to the groups listing screen, shown in Figure 3.

3 Provider Object ACLs

3.1 Granting Provider Object ACL Permissions

3.1.1 Design Overview

As previously mentioned, the Provider's *Administrators* group will be initially granted permissions on all Provider Objects and Catalog Items. This group will also have the ability to grant these privileges to all groups within their provider. The ability to grant privileges, however, may not be passed on. Only the ECHO Operations System Administrators group may control that ability.

3.1.2 User Interface

Select "Provider Object ACLs" under "Data Management" and the screen shown in Figure 5 will be displayed. The user is presented with a list of groups for which they may view or update ACLs. Select the appropriate group from the select list and press the "View/Manage Acls" button. The screen shown in Figure 6 will be displayed.

After making changes to the available provider object ACL permissions, press 'Save' to update the group's permissions.

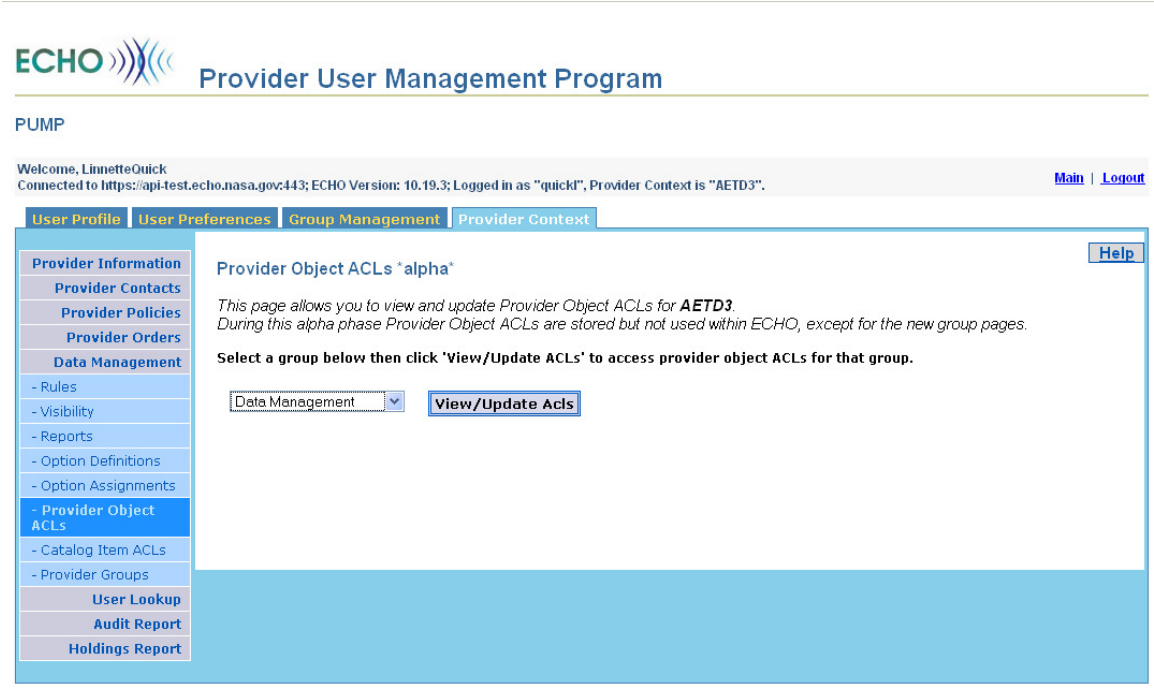


Figure 5 - Provider Object ACLs - Group Listing

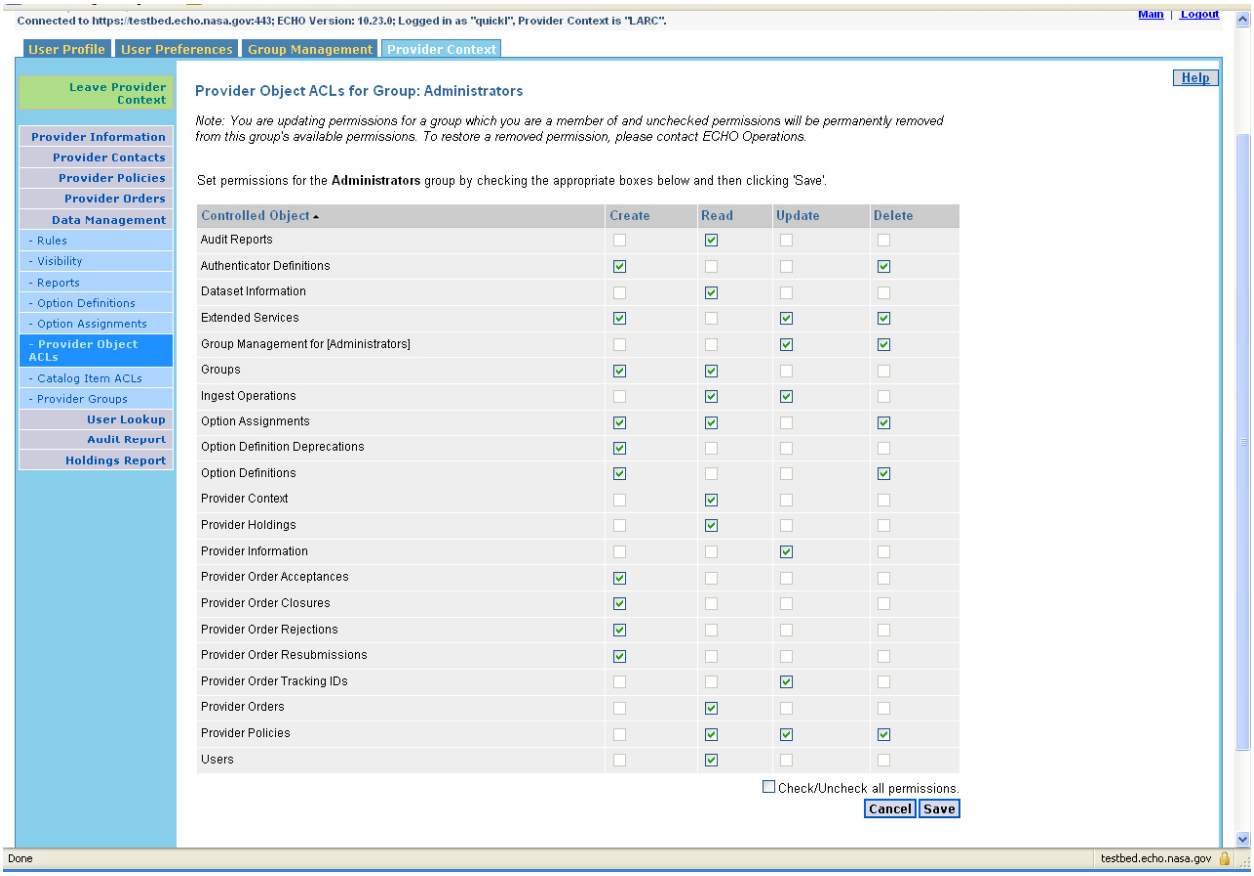


Figure 6 - Provider Object ACLs - Managing ACL Permissions

3.1.3 Sample Use Case

A provider wishing to create a Data Management role could grant the following permissions allowing them to perform relevant activities.

- **Audit Reports** – Read
- **Provider Context** - Read
- **Dataset Information** – Read
- **Groups** – Create & Read
- **Ingest Operations** – Read & Update
- **Provider Holdings** – Read
- **Provider Policies** – Create, Read, Update, & Delete

3.1.4 EIAT Management

Providers will manage access to the EIAT by granting “Read & Update” for the “Ingest Operations” Controlled Object to the appropriate groups.

4 Catalog Item ACLs

4.1 Creating Catalog Item ACLs

4.1.1 Design Overview

Catalog Item ACLs are applied to a static or dynamic listing of collections and/or granules. To create an ACL which manages access to collections, collections may be identified using the following mechanisms:

- Static list of selected collections
- Dynamic listing of collections based on Dataset ID, ShortName, and/or Version ID pattern matching.
- All collections
- Temporal Field Filtering
- Restriction Flag Filtering

To create an ACL which manages access to granules, granules may be identified using the following mechanisms:

- Owning collection identifiers, as listed above
- Temporal Field Filtering
- Restriction Flag Filtering
- Granule UR Filtering

4.1.2 User Interface

Select “Catalog Item ACLs” under “Data Management” and the screen in Figure 7 will be displayed. The user is presented with a list of the current catalog item ACLs. Select the “Add Catalog Item ACL” button. The screen shown in Figure 8 will be displayed.

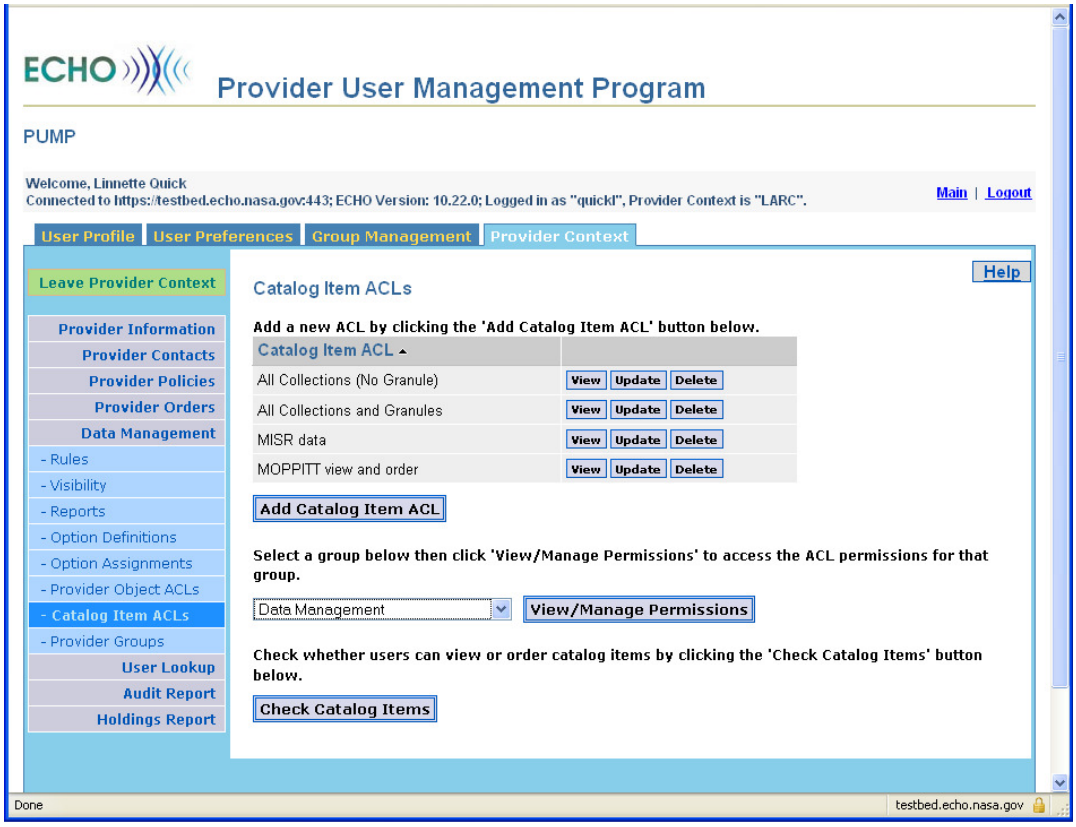


Figure 7- Catalog Item ACLs - Group Listing

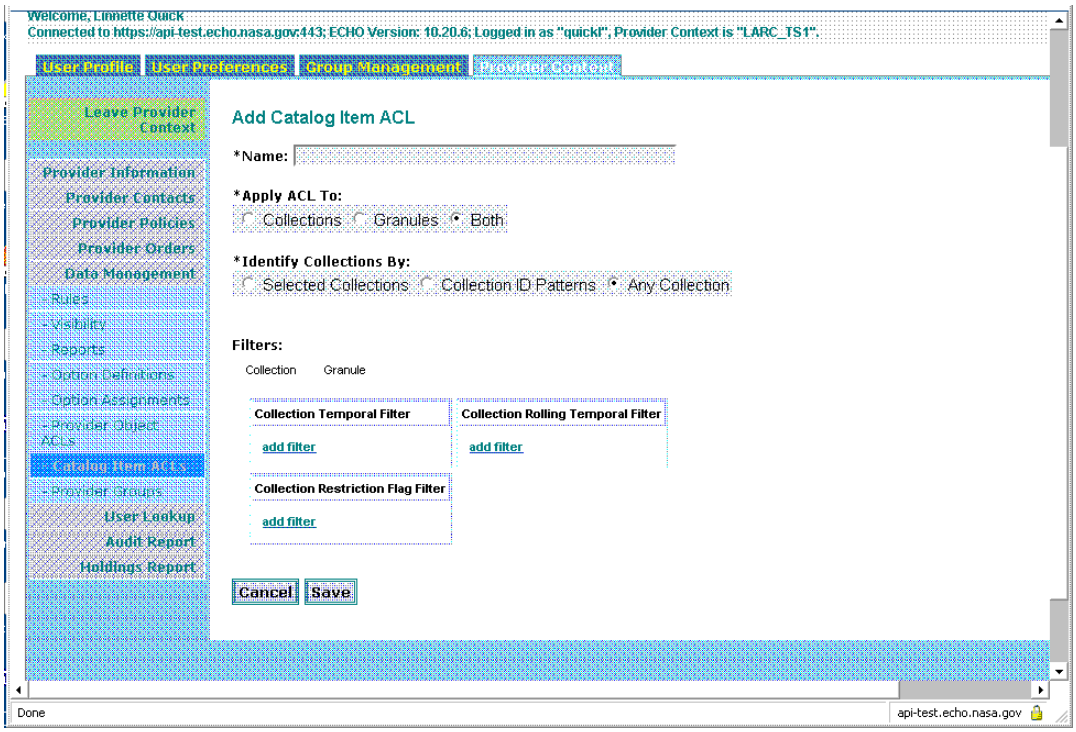


Figure 8 - Catalog Item ACLs – Add

Under the heading "*Identify Collections By:" collections can be identified using the following filters.

- Selected Collections – Choose collection(s) that will be included from the list of collections.
- Collection ID Patterns – Collection(s) can be indentified using the "Data Set ID" and/or "Short Name" and/or "Version ID". Only simple patterns are supported (not full regular expressions) using the "%" and "_" wildcard characters. For example, "MISR%" will match any string starting with the text 'MISR' and "M_ISR" will match any string whose 1st, 3rd, 4th and final characters are "M", "I","S" and "R" respectively.
- Any Collection – All of the collections will be included.

An example using all of the filters for "Collection ID Patterns" is shown below in Figure 9.

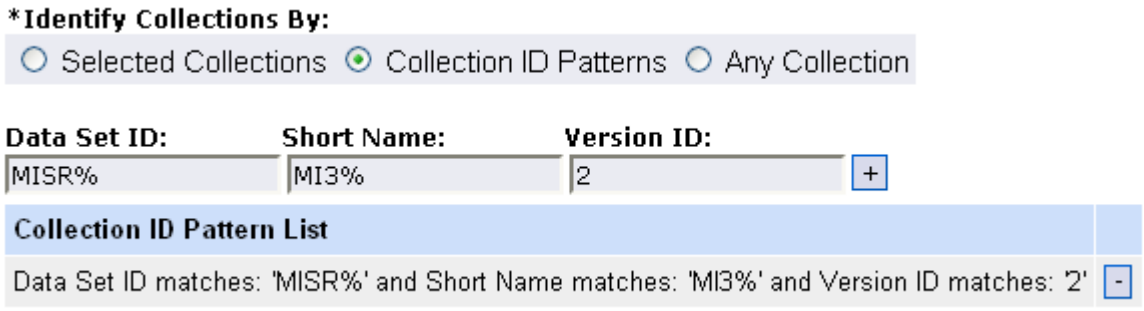


Figure 9 - Catalog Item ACL – Collection ID Patterns

4.1.3 Sample Use Case

Provider creates an ACL for Data Set ID(s) that match the pattern "MISR%" with the Short Name(s) matching the pattern "MI3%" for Version ID of 2.

4.2 Catalog Item Filters

4.2.1 Temporal Filters

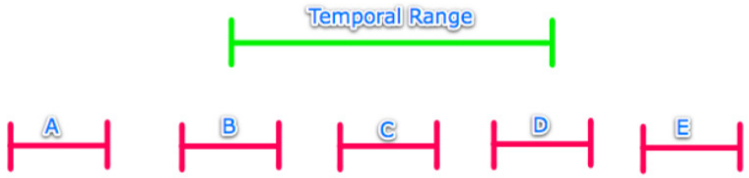
Temporal filters are created to specify the date range that the following granule or collection date fields will be matched against:

- **Acquisition Date** – From the collection or granule <Temporal> element. This is often a range value, not a single date and time.
- **Production Date** – From the <DataGranule> granule element. (Not available for collection filtering)
- **ECHO Insert Date** – The date that the collection or granule was inserted into ECHO.
- **ECHO Last Update Date** – The date that the collection or granule was last updated (inserted, replaced, or partially updated) in ECHO.

Temporal filtering may be performed using three comparator methods. A combination of these three methods may be used to construct any temporal filtering needs. The comparator methods will apply to granules or collections according to the following rules.

- **Intersect**– The specified filter range overlaps with the specified date value or range.
- **Contains**– The specified filter range contains the specified date value or range.
- **Disjoint** – The specified filter range does not overlap with the specified date value or range.

The following images illustrate how ECHO will perform temporal filtering using graphical examples.

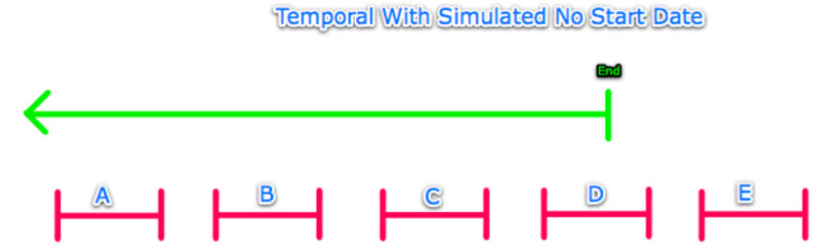


This table contains a Y if the above temporal range combined with the matching method will permit the collection.

	Matches A?	Matches B?	Matches C?	Matches D?	Matches E?
INTERSECT	N	Y	Y	Y	N
CONTAINS	N	N	Y	N	N
DISJOINT	Y	N	N	N	Y

Temporal No Start Date

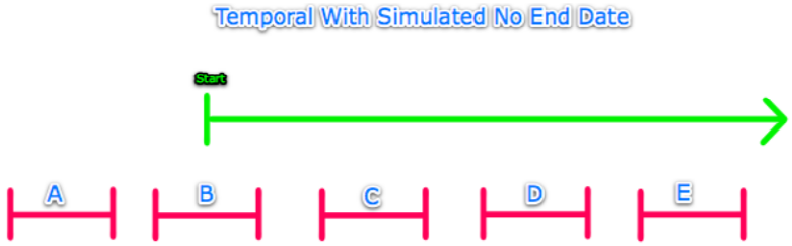
A temporal filter with no start date can be simulated by using a very early date (before any data could have existed).



	Matches A?	Matches B?	Matches C?	Matches D?	Matches E?
INTERSECT	Y	Y	Y	Y	N
CONTAINS	Y	Y	Y	N	N
DISJOINT	N	N	N	N	Y

Temporal No End

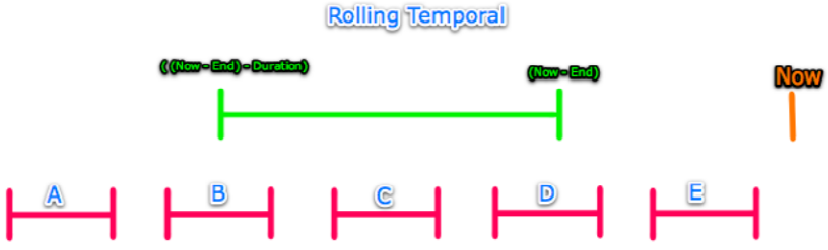
A temporal filter with no end date can be simulated by using a date far into the future.



	Matches A?	Matches B?	Matches C?	Matches D?	Matches E?
INTERSECT	N	Y	Y	Y	Y
CONTAINS	N	N	Y	Y	Y
DISJOINT	Y	N	N	N	N

RollingTemporalFilter

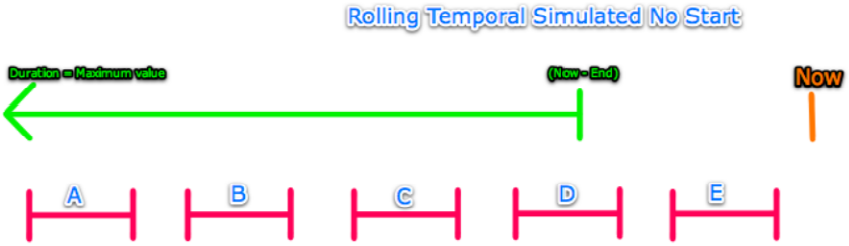
- RollingTemporalFilter
  - Temporal Field - (PRODUCTION, ACQUISITION, ECHO_LAST_UPDATE, ECHO_INSERT)
  - End - Number of milliseconds before now that the rolling temporal period will end at.
  - Duration - Number of milliseconds of duration for the rolling temporal period.
  - Matching Method - (INTERSECT, CONTAINS, DISJOINT)



	Matches A?	Matches B?	Matches C?	Matches D?	Matches E?
INTERSECT	N	Y	Y	Y	N
CONTAINS	N	N	Y	N	N
DISJOINT	Y	N	N	N	Y

Rolling Temporal With No Start Date

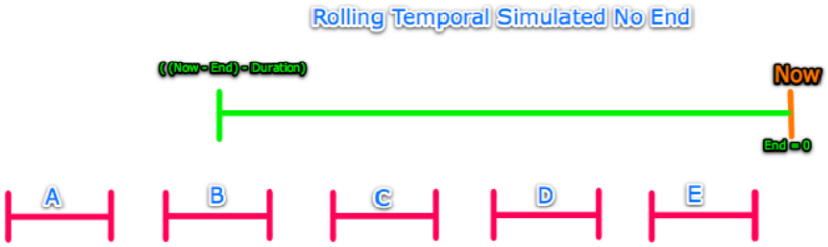
A rolling temporal filter with no start date can be simulated by setting Duration to the maximum value possible.



	Matches A?	Matches B?	Matches C?	Matches D?	Matches E?
INTERSECT	Y	Y	Y	Y	N
CONTAINS	Y	Y	Y	N	N
DISJOINT	N	N	N	N	Y

Rolling Temporal With No End Date

A rolling temporal filter with no end date can be simulated by setting End to 0.



	Matches A?	Matches B?	Matches C?	Matches D?	Matches E?
INTERSECT	N	Y	Y	Y	Y
CONTAINS	N	N	Y	Y	Y
DISJOINT	Y	N	N	N	N

The screen shown in Figure 10 displays the temporal and rolling temporal filters which are available for collection filtering. The same options exist for granule filtering as well.

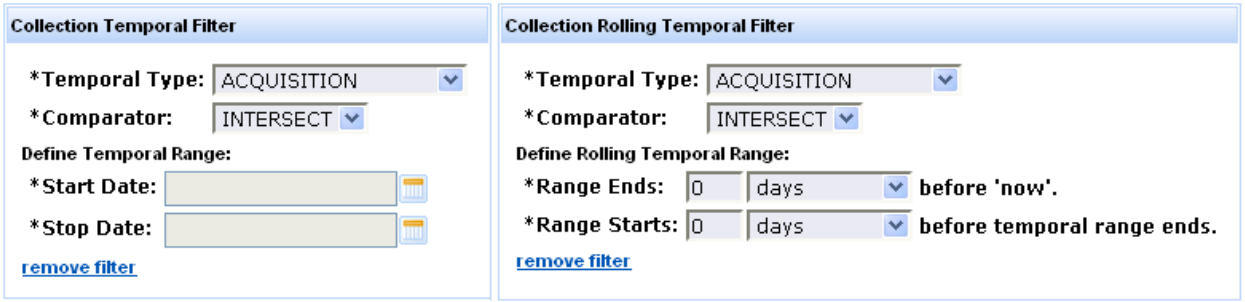


Figure 10 - Temporal & Rolling Temporal Filters

4.2.2 Restriction Flag Filters

Restriction flag filters are created to specify a range of values which a collection's or granule's restriction flag will be matched against. If a catalog item does not have a value for the restriction flag, then that item will be unaffected by the restriction flag filter.

4.2.3 Granule UR Filters

The Granule UR filter allows for a discrete list of granules to be included in an ACL filter. While performing catalog item filtering, each item in the list will be compared to determine whether the ACL should apply.

4.3 Granting Catalog Item ACL Permissions to Provider Groups

4.3.1 Design Overview

As previously mentioned, the Provider's Administrators group will be initially granted permissions on all Catalog Items. This group will also have the ability to grant these privileges to all groups within their provider. The ability the manage catalog item ACLs is transferrable to other groups, and will be explained further in the following section. This capability allows the user services team to manage access to a provider's data without coordination with ECHO Operations or the Provider Administrators group.

4.3.2 User Interface

Select "Catalog Item ACLs" under "Data Management" and the screen in Figure 11 will be displayed. The user is presented with a list of groups for which they may view or update ACLs. Select the appropriate group from the select list and press the "View/Manage Permissions" button. The screen shown in Figure 12 will be displayed.

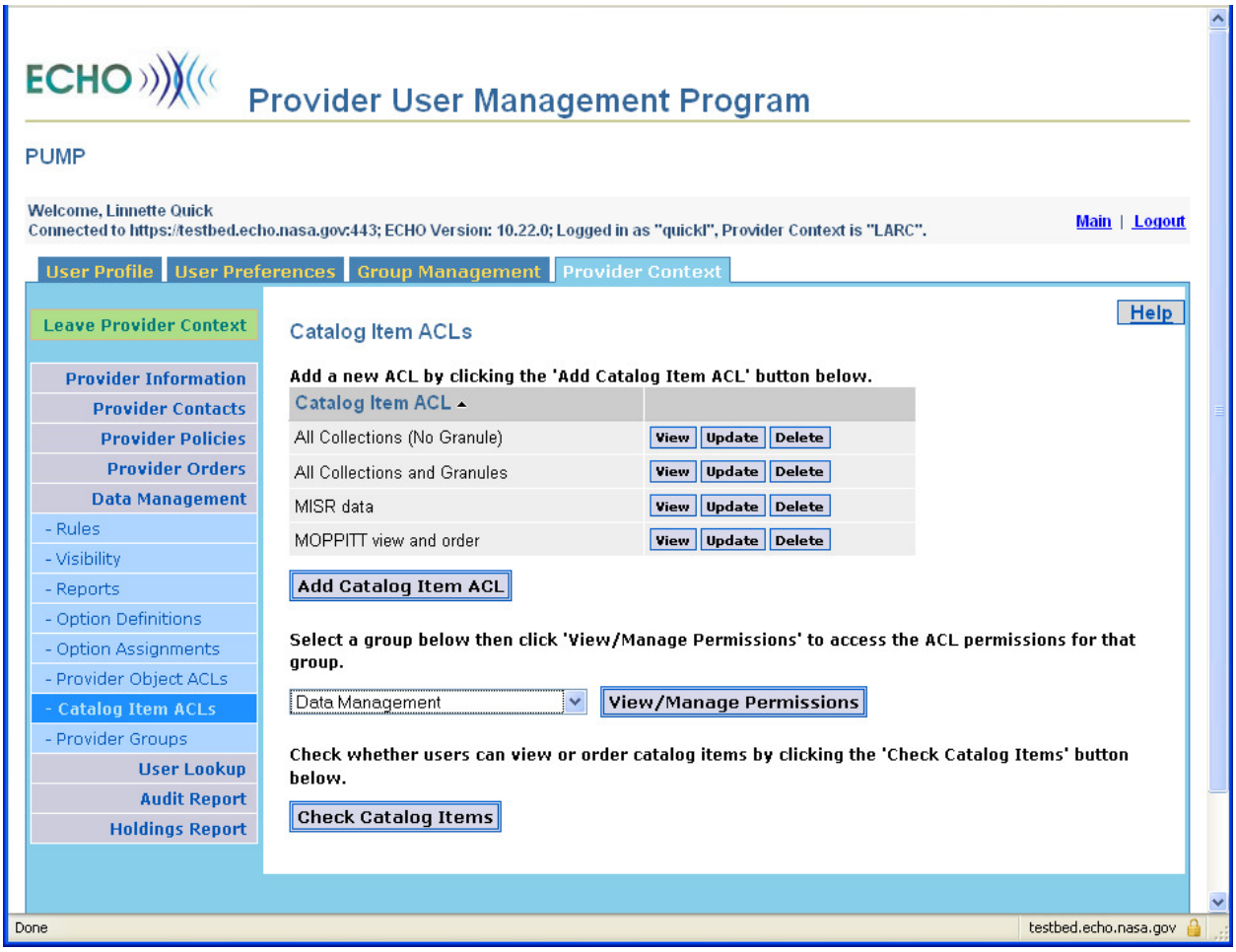


Figure 11 - Catalog Item ACLs – Group Listing

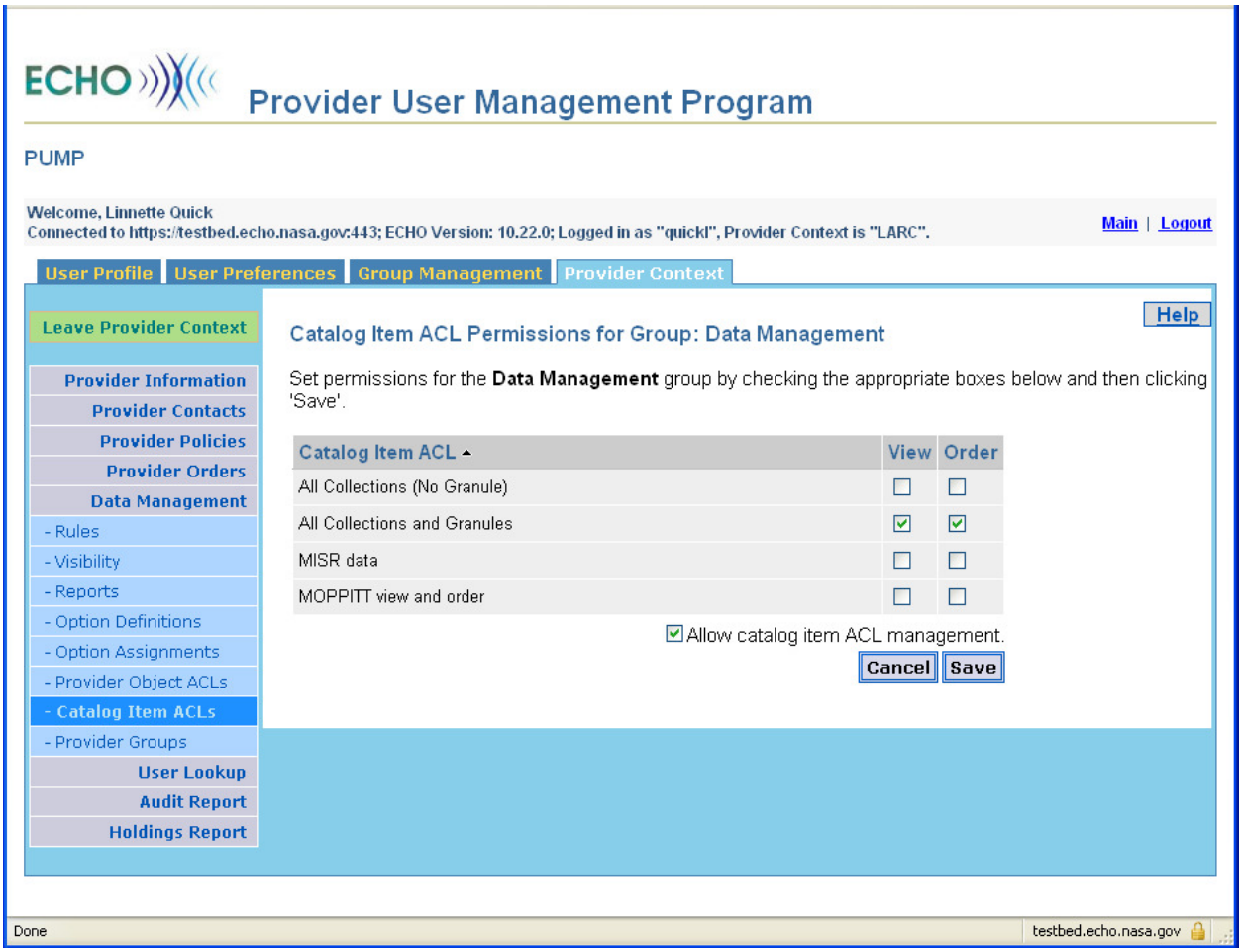


Figure 12 - Catalog Item ACLs - Managing ACL Permissions

The above screen displays all catalog item ACLs and the permissions assigned to the current group for those ACLs. An ACL may exist without having permissions assigned to a group, and that is acceptable. This simply indicates that the current group's catalog item access is unaffected by that ACL. The "All Collections (No Granule)" and "All Collections and Granules Catalog Item ACLs will be initially created for every provider.

Select "View" and/or "Order" check boxes to grant the current group permission to view and/or order the catalog items which are associated to the corresponding ACL. Selecting the "Allow catalog item ACL management" checkbox will allow the current group to change Catalog Item ACL permissions for other groups, create new Catalog Item ACLs, and delete any existing Catalog Item ACLs.

To finalize all changes, press the 'Save' button.

4.3.3 Sample Use Case

A provider wishing to create a Data Management role could grant the following permissions allowing them to perform relevant activities.

4.4 Granting Catalog Item ACL Permissions to Guest Users

4.4.1 Design Overview

Guest users are considered a “virtual group” in the new ACL and Group Management structure. This group is managed by the ECHO system dynamically to allow for public access to users who have not logged in to ECHO while discovering data. Each provider must manage the access level granted to guest users for their data holdings.

*NOTE – Guest User access and Registered User access must be configured separately.

4.4.2 User Interface

Select “Catalog Item ACLs” under “Data Management” and the screen in Figure 13 will be displayed. The user is presented with a list of groups for which they may view or update ACLs. Select the “Guest Users (System Group)” item from the drop-down menu and press the “View/Manage Permissions” button. The screen shown in Figure 14 will be displayed. As was previously discussed, select the permissions on the ACLs to which guest users should be granted access. To finalize all changes, press the 'Save' button.

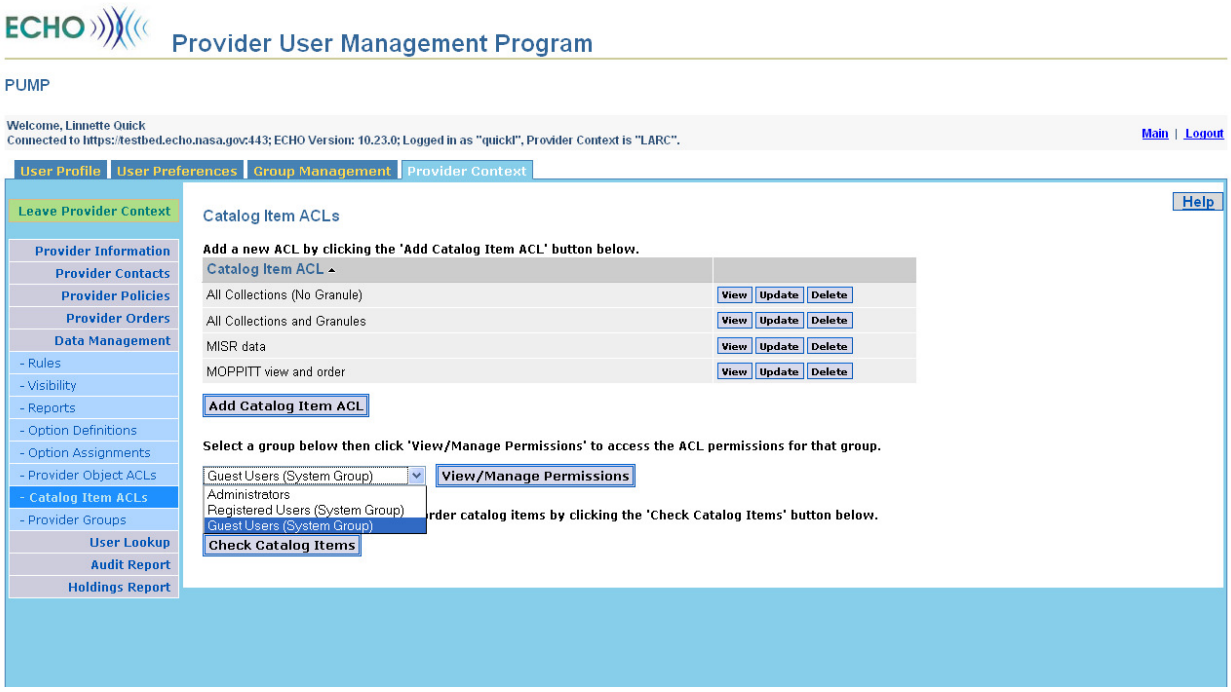


Figure 13 - Catalog Item ACLs - Guest User Permissions

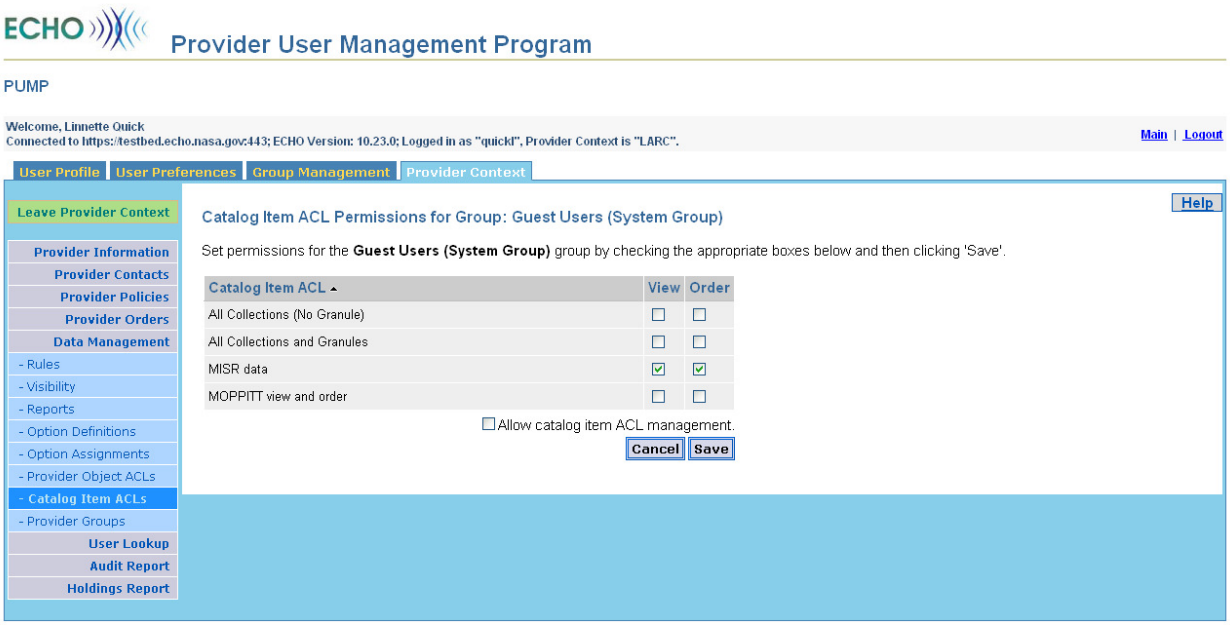


Figure 14 - Catalog Item ACLs - Managing ACL Permissions (Guests)

4.4.3 Sample Use Case

A provider will have a list of collections and granules that are generally available without any restrictions. ACLs should be created, and permissions assigned to the Guest Users group to allow for unrestricted access to guest users.

4.5 Granting Catalog Item ACL Permissions to Registered Users

4.5.1 Design Overview

Registered users are considered a “virtual group” in the new ACL and Group Management structure. This group is managed by the ECHO system dynamically to allow for public access to users who have logged in to ECHO while discovering data. Each provider must manage the access level granted to registered users for their data holdings.

*NOTE – Guest User access and Registered User access must be configured separately.

4.5.2 User Interface

Select “Catalog Item ACLs” under “Data Management” and the screen in Figure 15 will be displayed. The user is presented with a list of groups for which they may view or update ACLs. Select the “Registered Users (System Group)” item from the drop-down menu and press the “View/Manage Acls” button. The screen shown in Figure 16 will be displayed. As was previously discussed, select the permissions on the ACLs to which registered users should be granted access. To finalize all changes, press the 'Save' button.

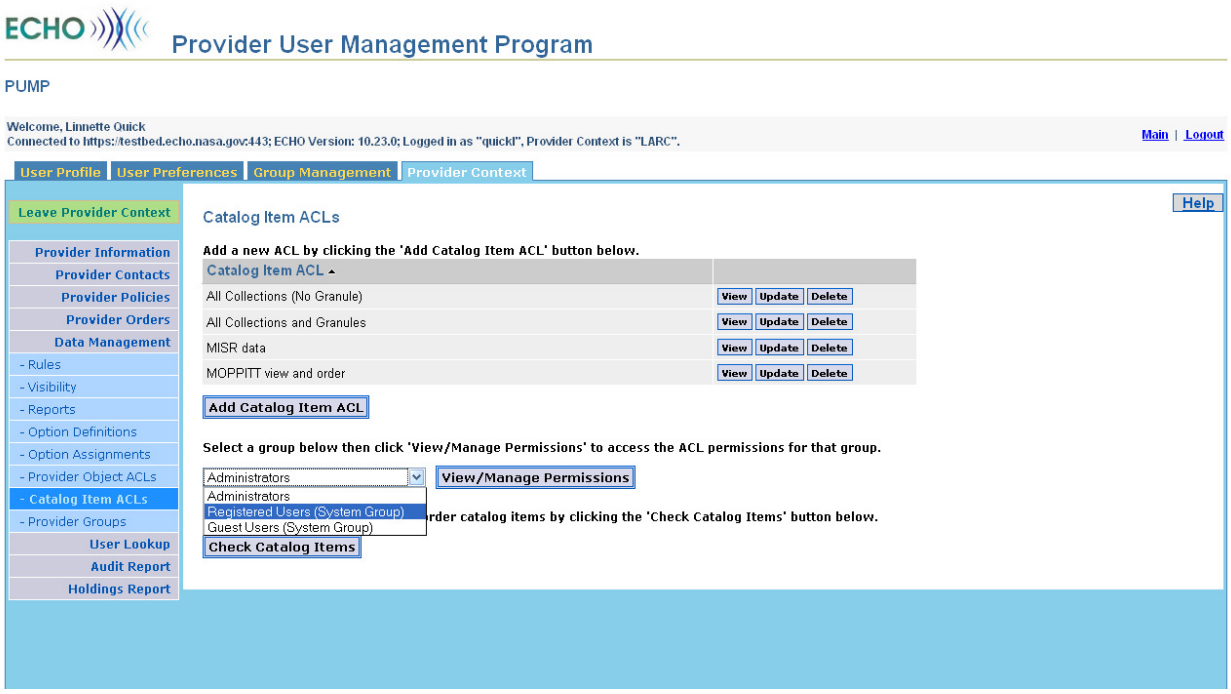


Figure 15 - Catalog Item ACLs - Group Listing

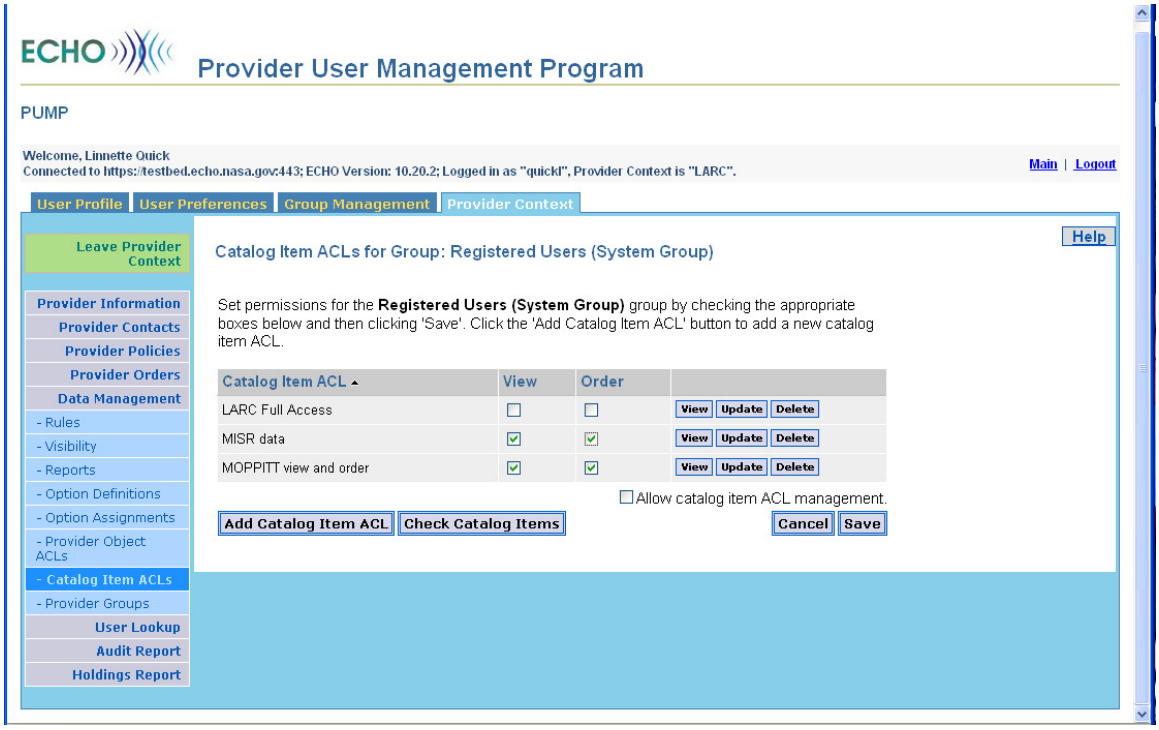


Figure 16 - Catalog Item ACLs - Managing ACL Permissions (Registered Users)

4.5.3 Sample Use Case

A provider will have a list of collections and granules that are generally available without any restrictions. ACLs should be created, and permissions assigned to the Registered Users group to allow for unrestricted access to registered users.

4.6 Checking View & Order Permissions for Registered Users

4.6.1 Design Overview

Registered Users must be granted permission to view and order catalog items. Providers can check whether a registered user has been granted permission for specific collections and/or granules.

4.6.2 User Interface

Select "Catalog Item ACLs" under "Data Management" and the screen in Figure 17 will be displayed. Press the "Check Catalog Items" to check view and order permissions for catalog items. The screen shown in Figure 18 will be displayed.

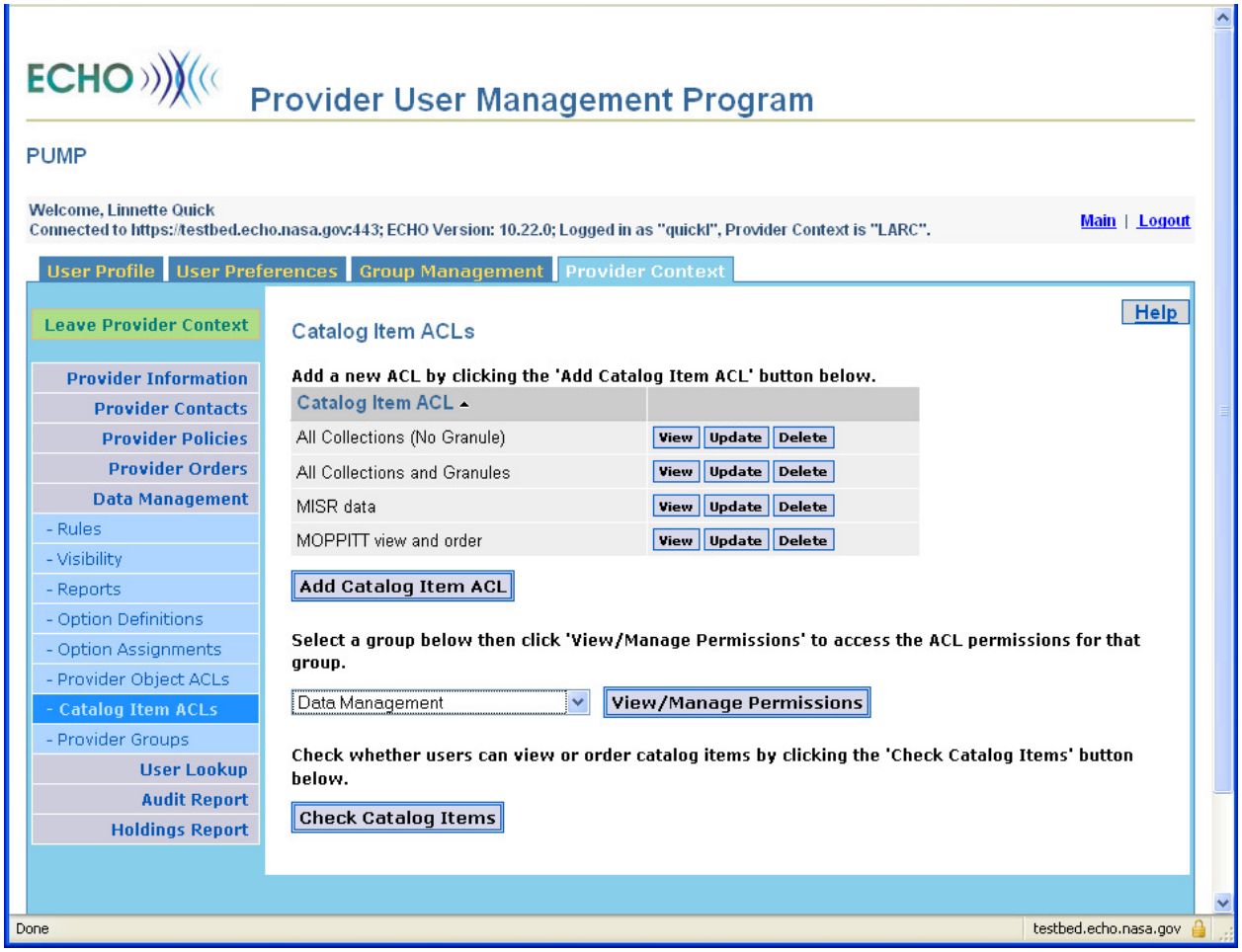


Figure 17 - Catalog Item ACLs – Check Catalog Items

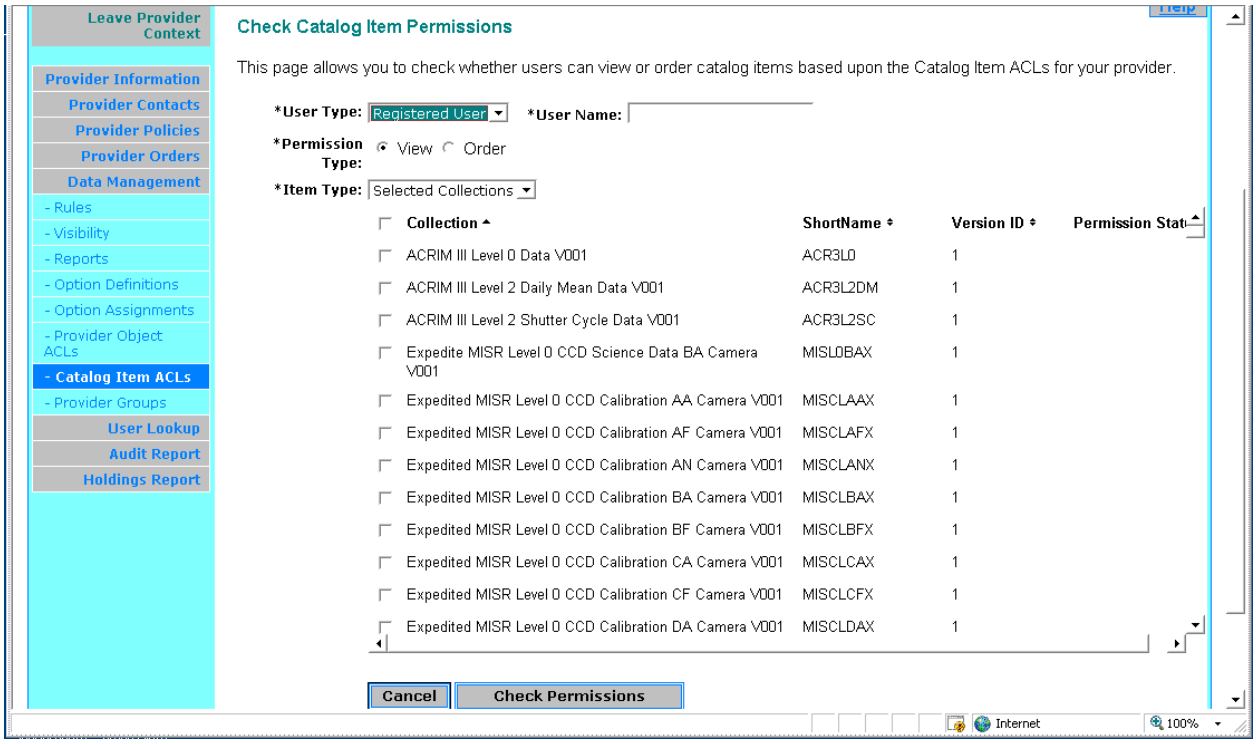


Figure 18 – Selected Collections – Registered User Check Permissions

The user is presented with a list of user types for which they may check permissions. Select the "registered user" type from the drop-down menu. Enter the registered user's name. Select "View" or "Order" for the "Permission Type". Select "Selected Collections" for the "Item Type". Select the desired collection(s) and press the "Check Permissions" button. The screen shown in Figure 19 will be displayed when checking "View" permissions. The screen shown in Figure 20 will be displayed when checking "Order" permissions.

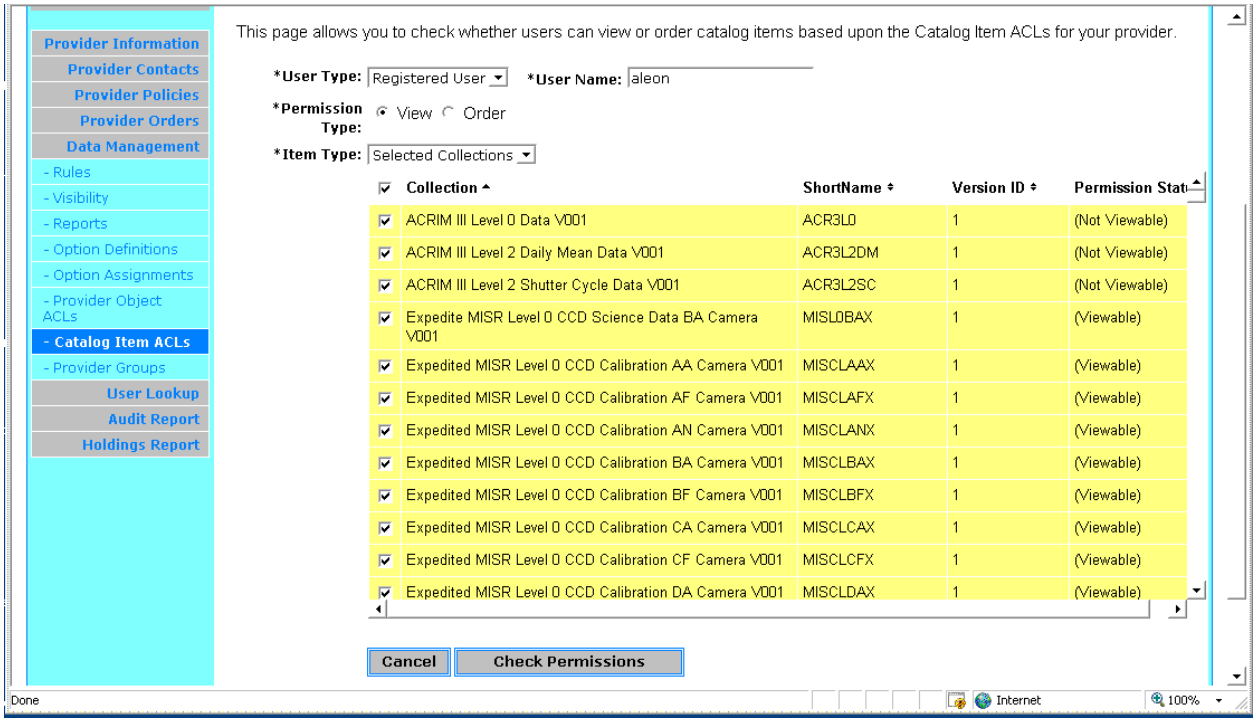


Figure 19 – Selected Collections – Registered User View Permission Result

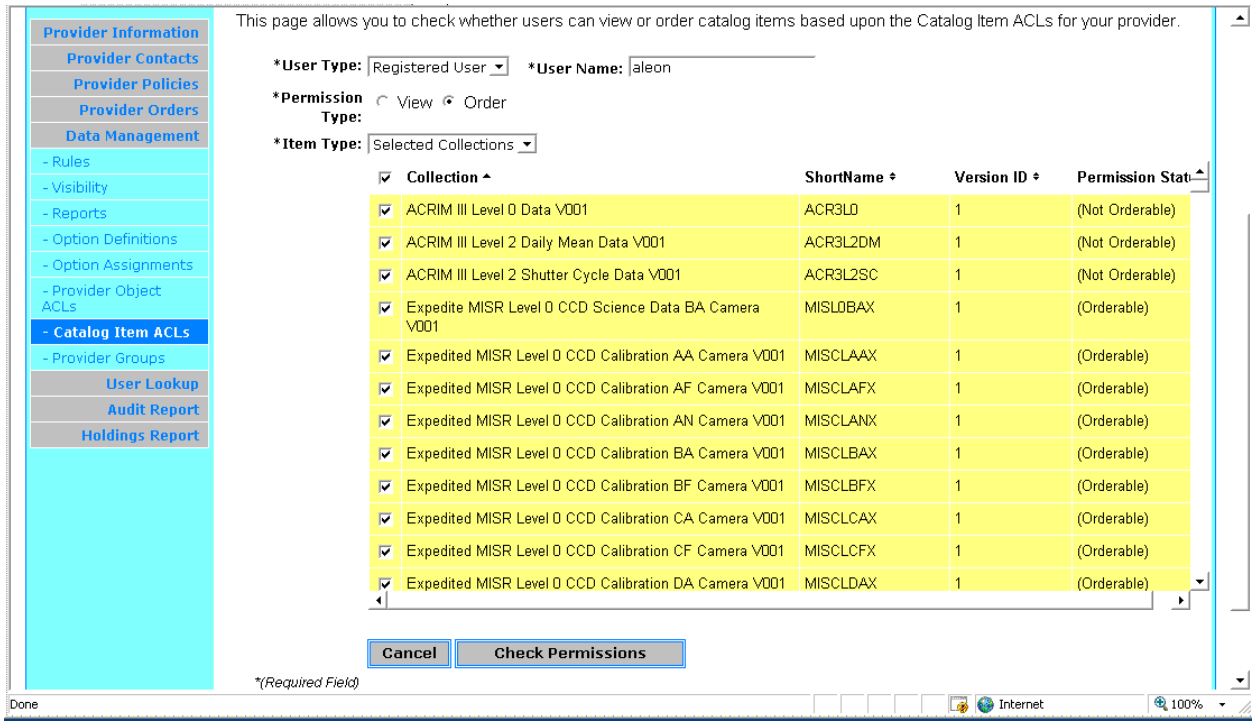


Figure 20 – Selected Collections – Registered User Order Permission Result

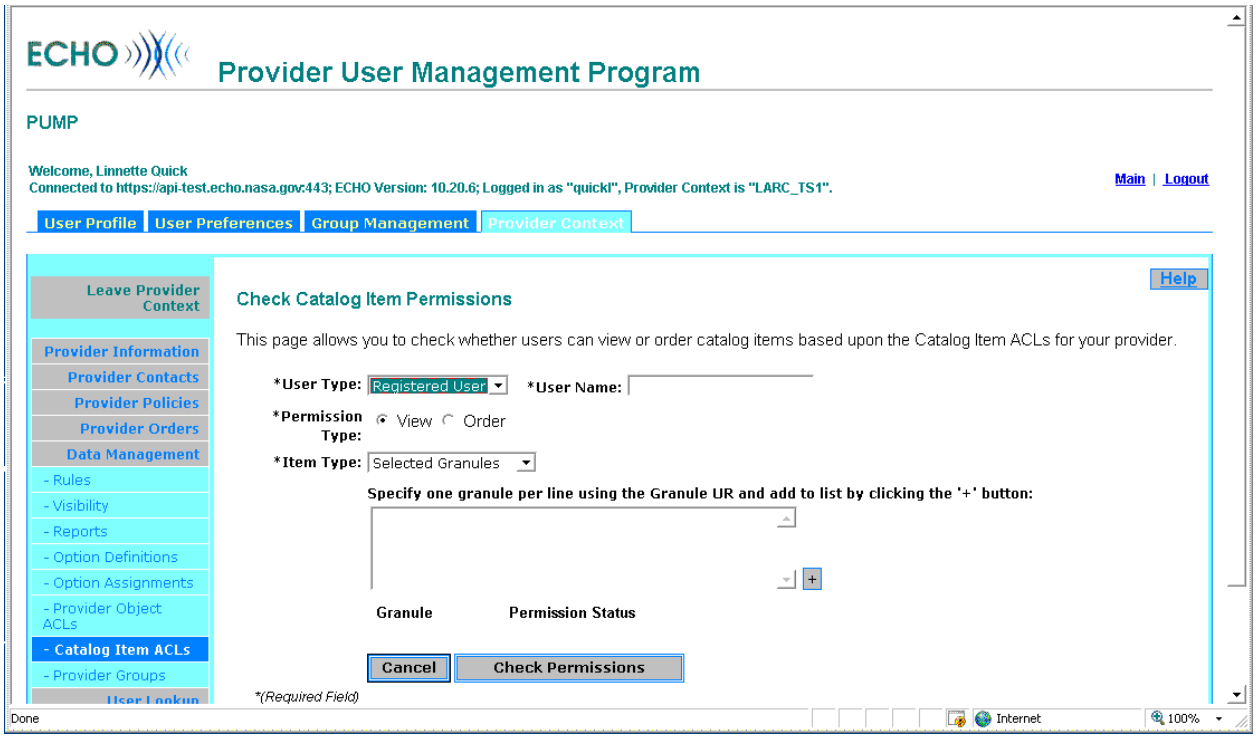


Figure 21 - Selected Granules - Registered User Check Permissions

The above screen allows providers to check view/order permissions for selected granules. Select the "registered user" type from the drop-down menu. Enter the registered user's name. Select "View" or "Order" for the "Permission Type". Select "Selected Granules" for the "Item Type". Enter one granule UR at a time then press the '+' button. Press the "Check Permissions" button. The screen shown in Figure 22 will be displayed when checking "View" permissions. The screen shown in Figure 23 will be displayed when checking "Order" permissions.

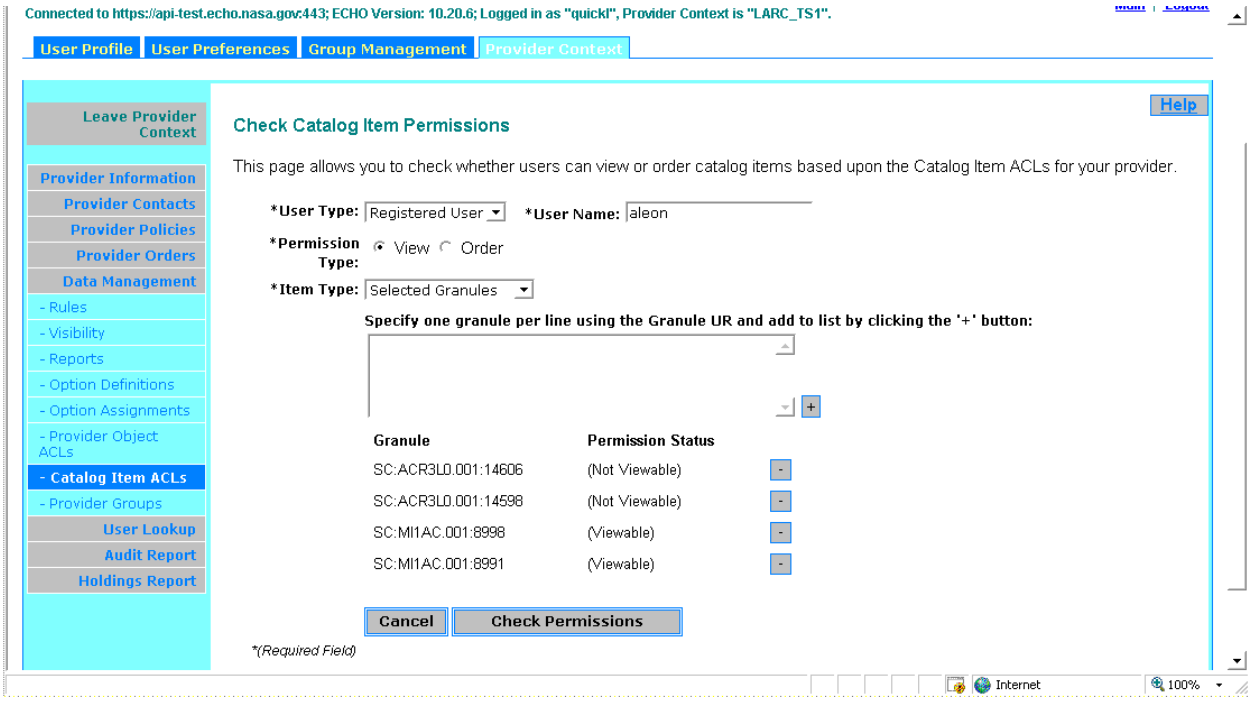


Figure 22 - Selected Granules - Registered User View Permission

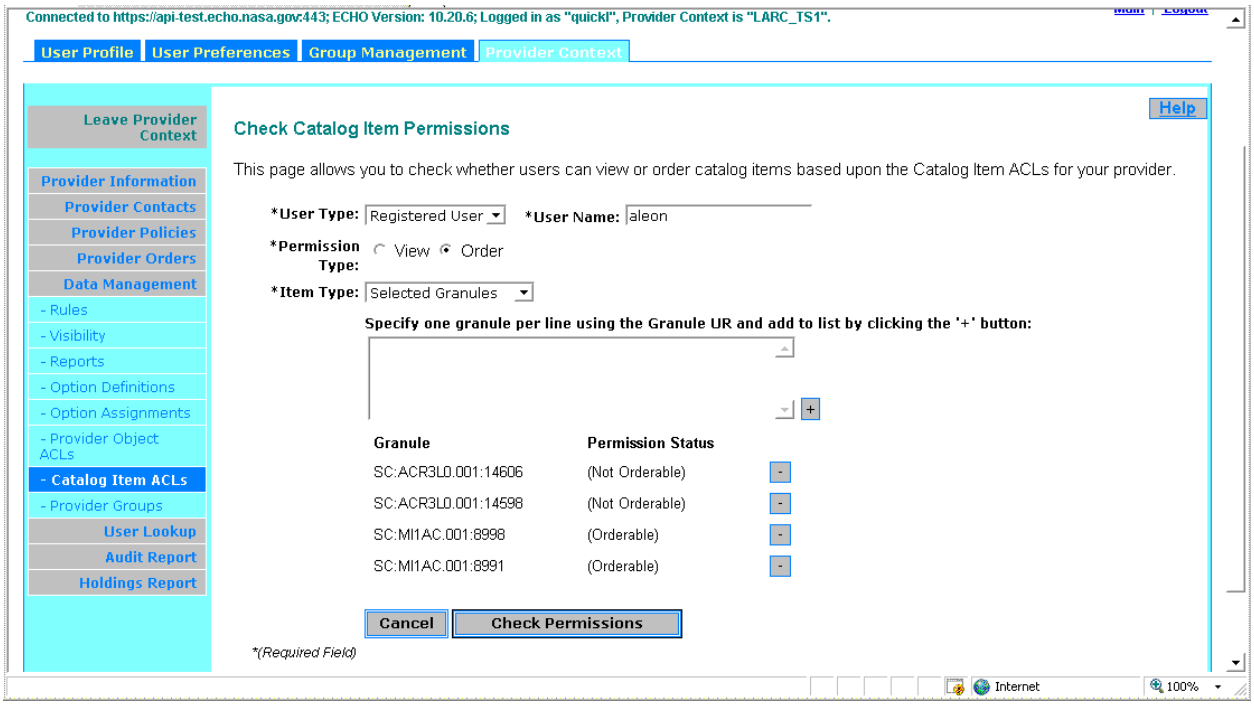


Figure 23 - Selected Granules - Registered User Order Permission

4.6.3 Sample Use Case

Registered Users group was granted view and order permission for all MISR and MOPPITT collections and granules. Registered Users group was restricted to view and order other collections.

4.7 Checking View & Order Permissions for Guest Users

4.7.1 Design Overview

Guest Users must be granted permission to view and order catalog items. Providers can check whether a guest user has been granted permission for specific collections and/or granules.

4.7.2 User Interface

Select "Catalog Item ACLs" under "Data Management" and the screen in Figure 24 will be displayed. Press the "Check Catalog Items" to check view and order permissions for catalog items. The screen shown in Figure 25 will be displayed.

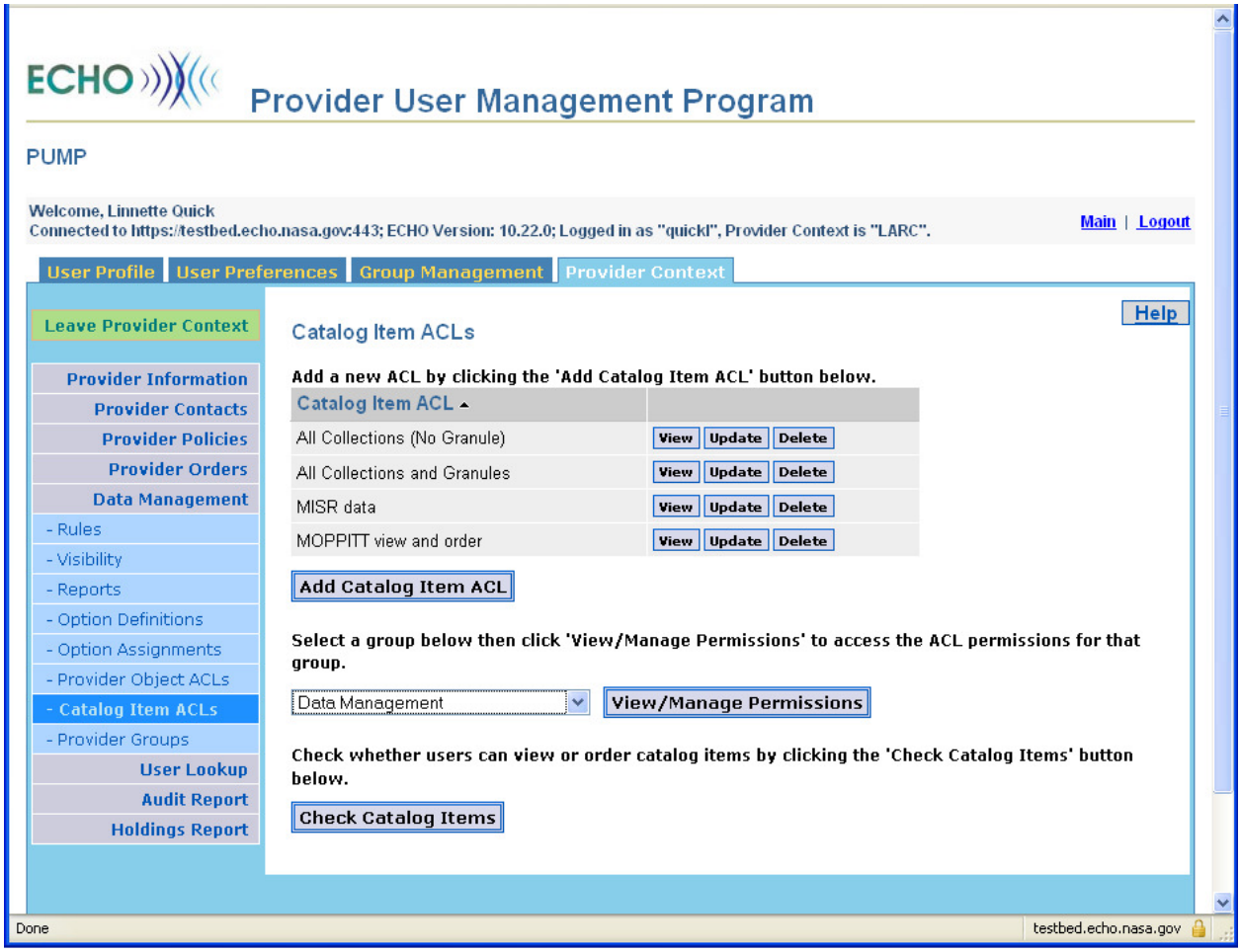


Figure 24 - Catalog Item ACLs - Check Catalog Items

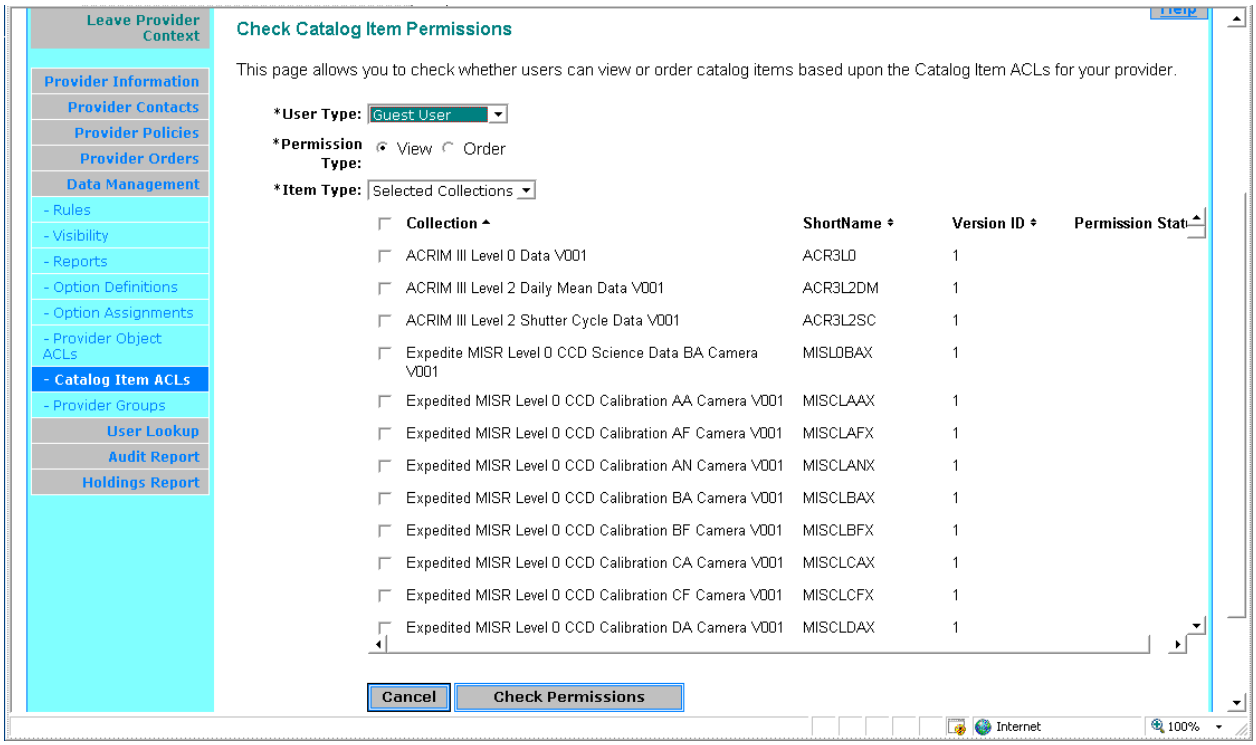


Figure 25 – Selected Collections - Guest User Check Permissions

The user is presented with a list of user types for which they may check permissions. Select the "guest user" type from the drop-down menu. Select "View" or "Order" for the "Permission Type". Select "Selected Collections" for the "Item Type". Select the desired collection(s) and press the "Check Read Permissions" button. The screen shown in Figure 26 will be displayed when checking "View" permissions. The screen shown in Figure 27 will be displayed when checking "Order" permissions.

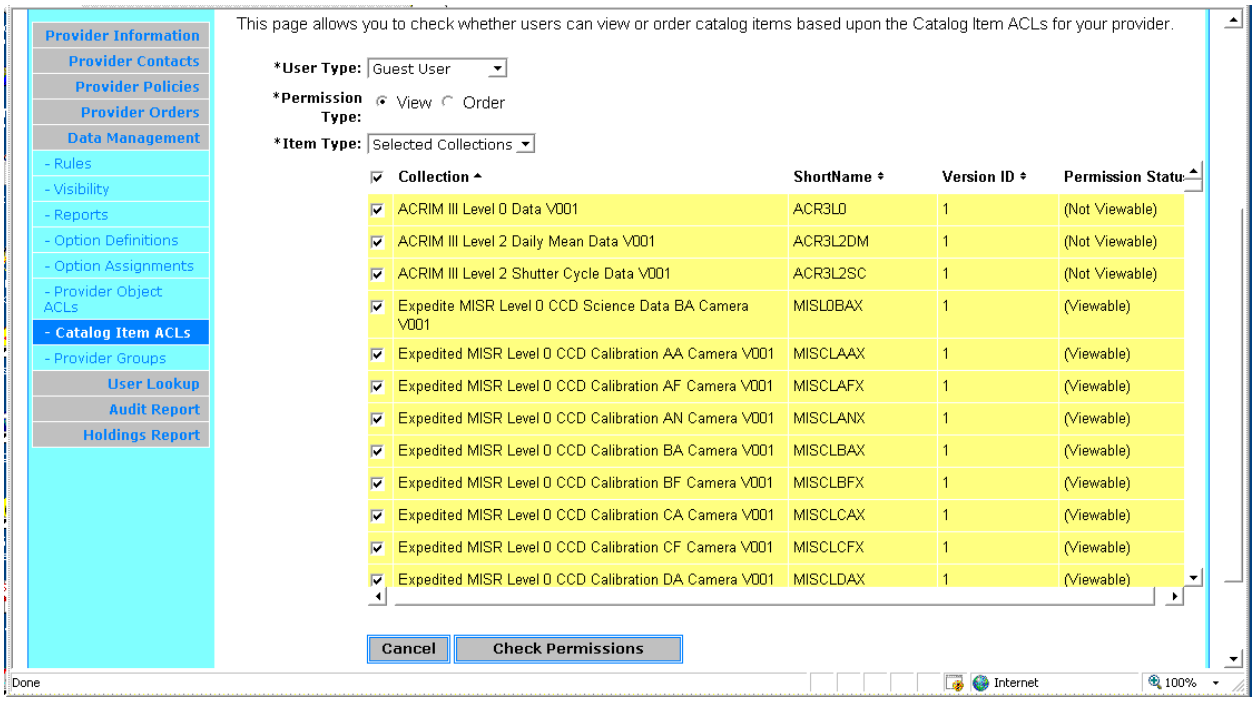


Figure 26 – Selected Collections - Guest User View Permission Result

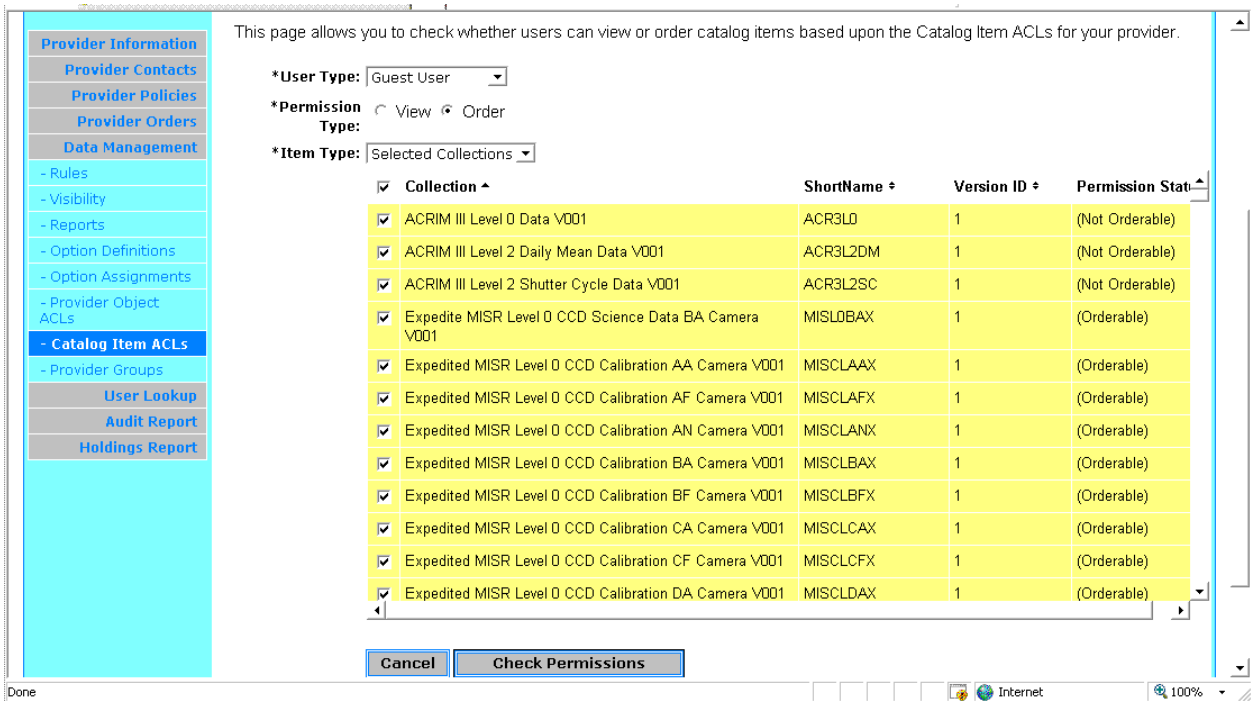


Figure 27 – Selected Collections - Guest User Order Permission Result

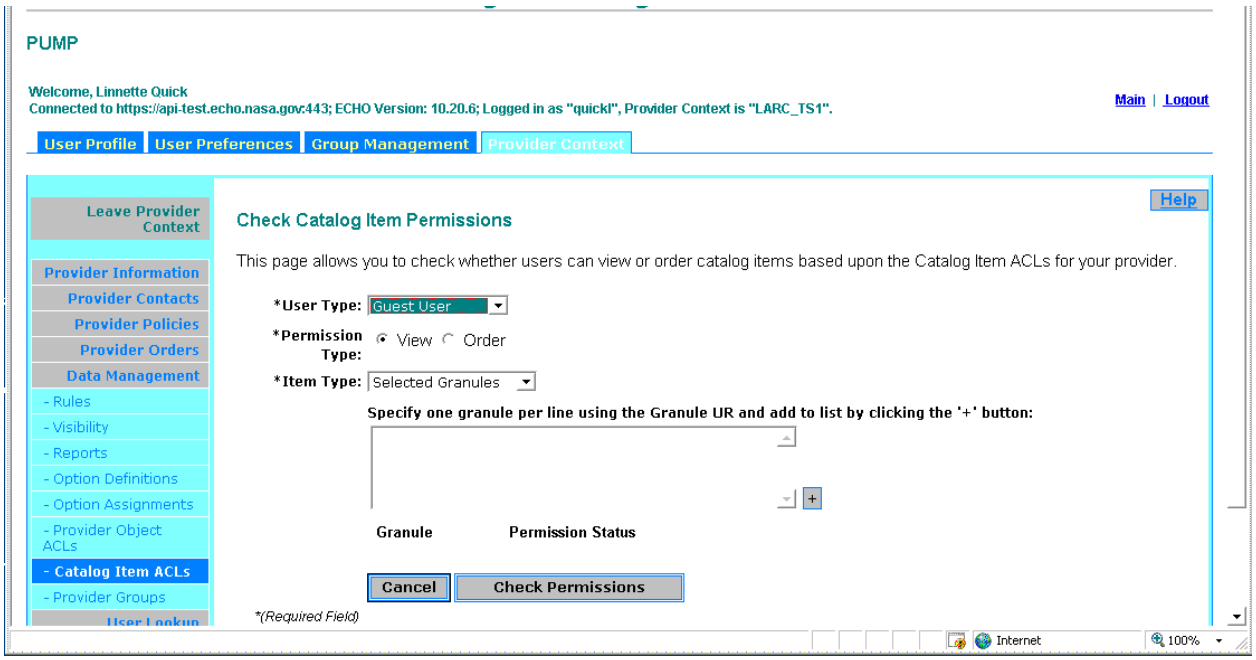


Figure 28 - Selected Granules - Check Permissions

The above screen allows providers to check view/order permissions for selected granules. Select the "guest user" type from the drop-down menu. Select "View" or "Order" for the "Permission Type". Select "Selected Granules" for the "Item Type". Enter one granule UR at a time then press the '+' button. Press the "Check Permissions" button. The screen shown in Figure 29 will be displayed when checking "View" permissions. The screen shown in Figure 30 will be displayed when checking "Order" permissions.

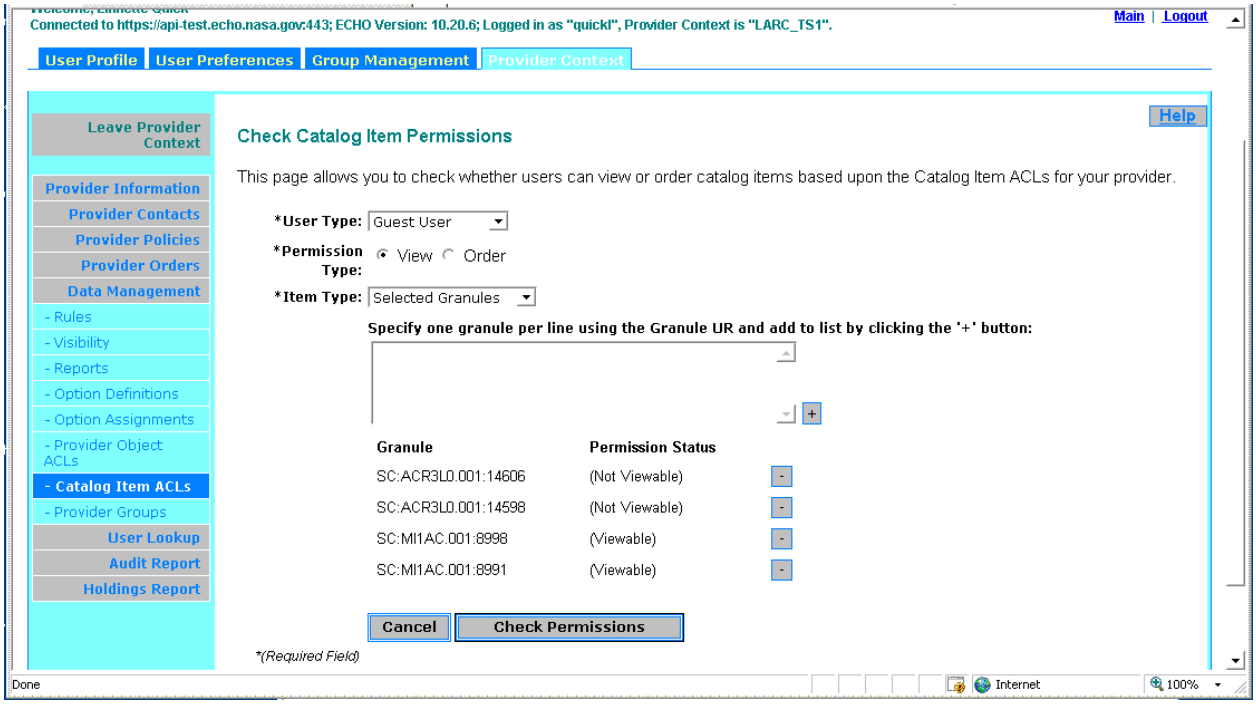


Figure 29 - Selected Granules - Guest User View Permission

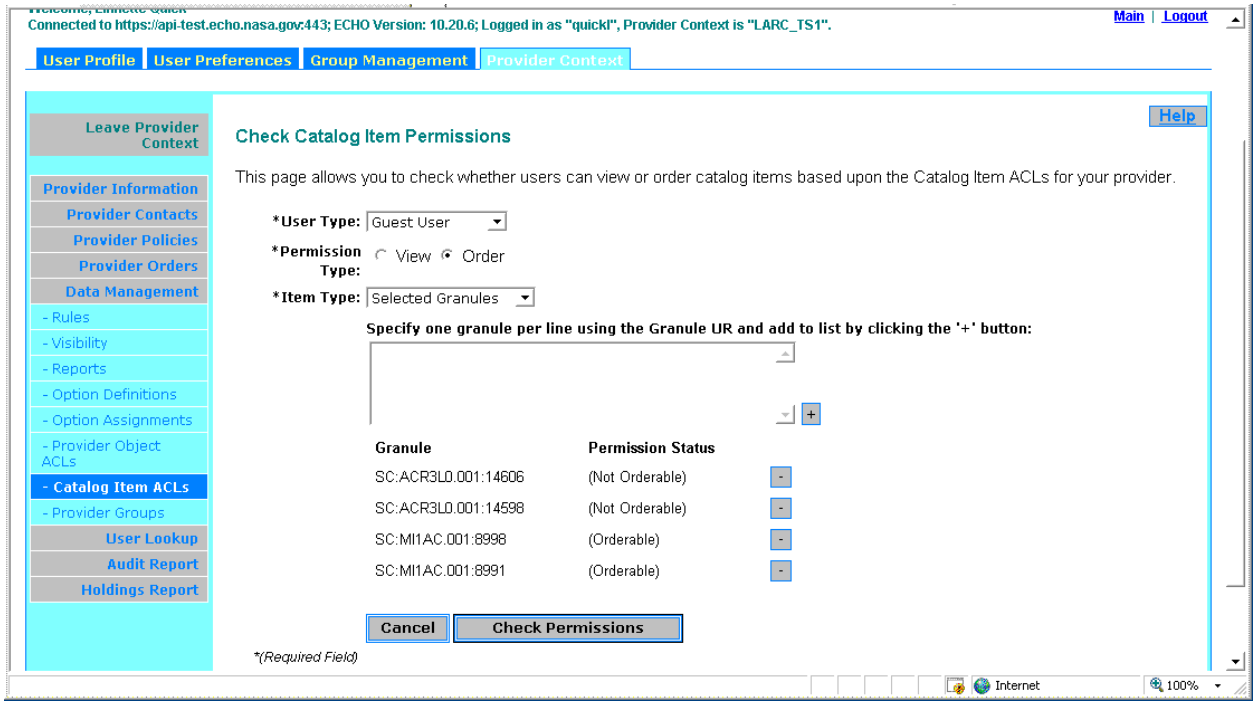


Figure 30 - Selected Granules - Guest User Order Permission

4.7.3 Sample Use Case

Guest User group was granted view and order permission for all MISR collections and granules. Guest User group was restricted to view and order other collections.

5 Catalog Item ACLs Working Example (NSIDC_ECS)

The NSIDC_ECS provider operational groups and ACLs were reviewed to suggest new groups and ACLS for ECHO 10.20. These are only suggestions based on the current descriptions.

5.1 Creating Groups

The first step in moving to the new Group and ACL management functionality is to determine which groups will be needed. The following table lists the current NSIDC_ECS groups which are being used in ACLs. The existing group's name and description are given, along with a proposed group name. Note that the new groups will be provider specific, so they do not need to be designated with the provider's name (e.g. NSIDC Ops, NSIDC Testers). In the case where new groups are being created, there is no existing group name.

Existing Group Name	Description	Proposed Group Name
	Users with provider role	Administrators
	Users that will create and manage Provider Object ACLs	Data Managers
	Users that will create and manage Catalog Item ACLs	User Services
ADEOS-II/AMSR Approved Users	Users with NASA approval to order JAXA's AMSR data.	ADEOS-II/AMSR Approved Users
MODIS Golden Month Approved Users	Users who have been approved to search and order MODIS Golden Month data.	MODIS Approved Users
NSIDC Testing	Allows internal staff to search and order any NSIDC data in ECHO	Testers
NSIDC_OPS_Test	NSIDC Operations team	DAAC Operations
WIST_Valids	ECHO Ops managed group for the WIST Valids user.	Group will no longer be visible to the provider.
ECHO_Operations	ECHO Ops managed group for the ECHO Ops team members.	Group will no longer be visible to the provider.

Table 1 - NSIDC_ECS Group Example

5.2 Creating ACLs

The second step in moving to the new Group and ACL Management functionality is to define the ACLs that will be needed. Table 2 lists the current NSIDC_ECS Operational ACLS. Table 3 lists the new ACLs that will be created. Note that these ACLs currently just define the data to which permissions are being granted. An ACL may exist without any groups having assigned permissions.

Description	Rule Type	Action Type	Target Item(s)
Allow NSIDC Ops to view all collections	Permit	View	All Collections
Allow NSIDC Testers to order all collections	Permit	Order	All Collections
Allow ordering of public collections	Permit	Order	Collection Listing
Allow ordering of AMSR/ADEIS-II data to approved users	Permit	Order	Collection Listing
Allow ordering of MODIS Golden Month data to approved users	Permit	Order	Collection Listing
Allow NSIDC Testers to view all collections	Permit	View	All Collections
Allow viewing of public collections	Permit	View	Collection Listing
Allow WIST_Valids to view all collections	Permit	View	All Collections
Allow ECHO Operations to view all collections	Permit	View	All Collections
Allow viewing of MODIS Golden Month data to approved users	Permit	View	Collection Listing
Restrict viewing to all collections	Restrict	View	All Collections
Restrict ordering to all collections	Restrict	Order	All Collections

Table 2 – Current NSIDC_ECS ACLs

ACL Name	ACL Applies To	ACL Selected Data
All Collections	Collections Only	All Collections
All Granules	Granules Only	All Collections
Public Collections	Collections Only	Selected Collections
Public Granules	Granules Only	Selected Collections
AMSR/ADEIS-II Collections	Collections Only	Selected Collections
AMSR/ADEIS-II Granules	Granules Only	Selected Collections
MODIS Golden Month Collections	Collections Only	Selected Collections
MODIS Golden Month Granules	Granules Only	Selected Collections

Table 3 – Proposed NSIDC_ECS ACLs

The previous table separates out collections from granules for each "type" of data (e.g. Public, AMSR). This is done in order to allow the provider to specify only the *view* permission to collections, but the *view* and *order* permissions to granules in those collections. If a provider would allow the metadata for these special (AMSR & MODIS) collections to be visible, then the "AMSR/ADEIS-II Collections" and "MODIS Golden Month Collections" ACLs would not be necessary.

5.2 Assigning Permissions

The final step in moving to the new Group and ACL Management functionality is to assign Catalog Item ACL permissions to the provider groups. The following table lists each proposed group and Catalog Item ACL, along with the assigned permissions.

Group Name	Administrators	Data Managers	User Services	DAAC Operations	Testers	ADEOS/AMSR Approved USers	MODIS Approved Users	Guest Users	Registered Users
All Collections	View	View	View	View	View				
All Granules	View & Order	View & Order	View & Order	View & Order	View & Order				
Public Collections								View	View
Public Granules								View & Order	View & Order
AMSR/ADEIS-II Collections						View			
AMSR/ADEIS-II Granules						View & Order			
MODIS Golden Month Collections							View		
MODIS Golden Month Granules							View & Order		

Table 4 – Proposed NSIDC_ECS ACL Permissions